

# COMPUTING INTEGRAL BASES VIA LOCALIZATION AND HENSEL LIFTING

JANKO BÖHM, WOLFRAM DECKER, SANTIAGO LAPLAGNE, AND GERHARD PFISTER

**ABSTRACT.** We present a new algorithm for computing integral bases in algebraic function fields, or equivalently for constructing the normalization of a plane curve. Our basic strategy makes use of localization and, then, completion at each singularity of the curve. In this way, we are reduced to finding integral bases at the branches of the singularities. To solve the latter task, we work with suitably truncated Puiseux expansions. In contrast to van Hoeij’s algorithm [21], which also relies on Puiseux expansions (but pursues a different strategy), we use Hensel’s lemma as a key ingredient. This allows us at some steps of the algorithm to compute factors corresponding to complete sets of conjugate Puiseux expansions, without actually computing the individual expansions. In this way, we make substantially less use of the Newton-Puiseux algorithm. In addition, our algorithm is inherently parallel. As a result, it outperforms in most cases any other algorithm known to us by far. Typical applications are the computation of adjoint ideals [4] and, based on this, the computation of Riemann-Roch spaces and the parametrization of rational curves.

## 1. INTRODUCTION

Let  $A$  be a reduced Noetherian ring, and let  $Q(A)$  be its total ring of fractions. The *normalization* of  $A$  is the integral closure of  $A$  in  $Q(A)$ . We denote the normalization by  $\bar{A}$  and call  $A$  *normal* if  $A = \bar{A}$ . Recall that if  $A$  is a reduced affine (that is, finitely generated) algebra over a field, then  $\bar{A}$  is a finite  $A$ -module by Emmy Noether’s finiteness theorem (see [13], [20]).

In this paper, we are interested in the case where  $A$  is the coordinate ring of an algebraic curve defined over a field  $K$  of characteristic zero. More precisely, let  $f \in K[X, Y]$  be an irreducible polynomial in two variables, let  $C \subset \mathbb{A}^2(K)$  be the affine plane curve defined by  $f$ , and let

$$A = K[C] = K[X, Y]/\langle f(X, Y) \rangle$$

be the *coordinate ring* of  $C$ . We write  $x$  and  $y$  for the residue classes of  $X$  and  $Y$  modulo  $f$ , respectively. Throughout the paper, we suppose that  $f$  is monic in  $Y$  (due to Noether normalization, this can always be achieved by a linear change of coordinates). Then the *function field* of  $C$  is of type

$$K(C) = Q(A) = K(x)[y] = K(X)[Y]/\langle f(X, Y) \rangle,$$

$x$  is a separating transcendence basis of  $K(C)$  over  $K$ , and  $y$  is integral over  $K[x]$ , with integrality equation  $f(x, y) = 0$ . In particular,  $A$  is integral over  $K[x]$ , which implies that  $\bar{A}$  coincides with the integral closure  $\bar{K}[x]$  of  $K[x]$  in  $K(C)$ . We may, hence, represent  $\bar{A}$  either by generators over  $A$  or by generators over  $K[x]$ . For the latter, note that  $\bar{A} = \bar{K}[x]$  is a free  $K[x]$ -module of rank

$$n := \deg_y(f) = [K(C) : K(x)].$$

Indeed, this follows by applying [19, Theorem 3.3.4] to the PID

$$K[x] \subset K(x) \subset K(C) = K(x)[y].$$

**Definition 1.1.** If  $R$  is any ring and  $B$  is a reduced Noetherian ring such that  $\bar{B}$  is a finite free  $R$ -module, then an *integral basis* for  $\bar{B}$  over  $R$  is a set  $b_1, \dots, b_r$  of free generators for  $\bar{B}$  over  $R$ :

$$\bar{B} = Rb_1 \oplus \dots \oplus Rb_r.$$

---

*Key words and phrases.* Normalization, integral closure, integral basis, curve singularity, Puiseux series.  
2010 Math subject classification: 13B22 (Primary) 14H20, 13P10, 13H99 (Secondary).

**Remark 1.2.** In the context outlined above, there is always an integral basis for  $\overline{A}$  over  $K[x]$  of type

$$1, \frac{p_1(x, y)}{d(x)}, \dots, \frac{p_{n-1}(x, y)}{d(x)},$$

with  $d \in K[x]$ , and with elements  $p_i \in K[x][y]$  of degree  $i$  in  $y$ . Such a basis is obtained from any given set  $1 = c_0, \dots, c_{m-1}$  of  $K[x]$ -module generators for  $\overline{A}$  by unimodular row operations over the PID  $K[x]$ : For each  $i$ , write  $c_i = \sum_{j=0}^{n-1} c_{ij} y^{n-1-j}$ , with coefficients  $c_{ij} \in K(x)$ . Then take  $d$  to be the least common denominator of the  $c_{ij}$ , transform the matrix  $(d \cdot c_{ij})$  into row echolon form  $(p_{ij})$ , and set  $p_{n-i} = \sum_{j=0}^{n-1} p_{ij} y^{n-1-j}$ , for  $i = 1, \dots, n-1$ .

**Remark 1.3.** General normalization algorithms are presented in [16], [5]. They are designed to return an ideal  $U \subset A$  together with an element  $d \in A$  such that  $\overline{A} = \frac{1}{d}U \subset Q(A)$ . Here, as we will recall in Section 2, any non-zero element of the Jacobian ideal  $M$  of  $A = K[x, y]$  can be taken to be  $d$ . In particular, we can choose  $d$  to be a generator of the elimination ideal  $M \cap K[x]$ . The roots of  $d$  in the algebraic closure  $\overline{K}$  of  $K$  are then precisely the  $x$ -coordinates of the singularities of the curve defined by  $f$  in  $\mathbb{A}^2(\overline{K})$ . If  $u_0 = d(x), u_1, \dots, u_r$  generate the ideal  $U$ , the  $y^i u_j(x, y)/d(x)$ ,  $0 \leq i \leq n-1$ ,  $0 \leq j \leq r$ , generate  $\overline{A}$  over  $K[x]$ . An integral basis is then obtained by operations as described in Remark 1.2.

**Remark 1.4.** In practical terms,  $u_0, \dots, u_r$  are given as polynomials in  $K[X, Y]$  of  $Y$ -degree at most  $n-1$ . If these polynomials, together with  $f$ , form a Groebner basis with respect to the lexicographical ordering, taking  $Y > X$ , then already the elements  $y^i u_j(x, y)/d(x)$ ,  $0 \leq i \leq n-1 - \deg(u_j)$ ,  $0 \leq j \leq r$ , generate  $\overline{A}$  over  $K[x]$ .

**Example 1.5.** Consider the standard cusp: Let

$$A = K[x, y] = K[X, Y]/\langle Y^3 - X^2 \rangle.$$

As a module over  $A$ , we may represent  $\overline{A}$  as

$$\overline{A} = A \cdot \frac{y^2}{x} + A \cdot 1 = \frac{1}{x} \langle y^2, x \rangle_A$$

(see [16, Example 2.5]). Considering  $\overline{A}$  over  $K[x]$ , we get

$$\overline{A} = K[x] \cdot \frac{y^2}{x} + K[x] \cdot y \cdot \frac{y^2}{x} + K[x] \cdot y^2 \cdot \frac{y^2}{x} + K[x] \cdot 1 + K[x] \cdot y + K[x] \cdot y^2.$$

Since  $y^3 = x^2$  and  $K[x] \cdot y^2 \subset K[x] \cdot y^2/x$ , we have

$$\overline{A} = K[x] \cdot \frac{y^2}{x} \oplus K[x] \cdot 1 \oplus K[x] \cdot y.$$

Hence,  $1, y, y^2/x$  is an integral basis as in Remark 1.2.

The algorithms in [16], [5] work for any reduced affine algebra  $A$  over a perfect field. They rely on the Grauert and Remmert normalization criterion which can be applied in a global or local setting (see [15], [17, Prop. 3.6.5], [5, Prop. 3.3]): Whereas the algorithm in [16] is of global nature, the idea in [5] is to consider a finite stratification of the singular locus  $\text{Sing}(A)$ , apply a local version of the normalization algorithm at each stratum, and find  $\overline{A}$  by putting the resulting local contributions together. If  $\text{Sing}(A)$  is finite, we may stratify it by considering each  $P \in \text{Sing}(A)$  separately. This applies, in particular, to the case where  $A = K[C]$  is the coordinate ring of a curve  $C$  as outlined above. As a consequence, computing an integral basis for  $A$  over  $K[x]$  is then equivalent to computing a local contribution to  $\overline{A}$  at each  $P$ .

In this paper, we present a new method for computing the local contributions which is custom-made for the case  $A = K[C]$ . We proceed along the following lines. To fix our ideas, in Sections 2 and 3, we briefly recall the Grauert and Remmert type algorithms. Furthermore, we discuss an efficient criterion for detecting whether a given point is the only singularity of the curve under consideration. In Section 4, we review the theory of Puiseux expansions and its connection to

integrality. In Section 5, taking an analytic point of view, we show how to obtain an integral basis at a given singularity  $P$  from integral bases at the branches of the singularity. In Section 6, we explain how to construct the local contribution at  $P$  from the integral basis at the singularity. How to actually find the integral bases at the branches is a topic of Section 7: Working with approximations by suitably truncated Puiseux series, we describe a way of writing down an integral basis for a single branch without performing too many computations. This approach is inspired by van Hoeij's paper [21], but pursues a different strategy, with Hensel lifting as a crucial new ingredient. Moreover, we modify the theoretical results of Section 5 in order to achieve a better performance.

We have implemented our algorithm in the open source computer algebra system SINGULAR [11]. In Section 8, we compare the performance of the algorithm with that of the local to global approach from [5]. We also give timings for the implementation of van Hoeij's algorithm in MAPLE and for the variant of the Round 2 algorithm implemented in MAGMA.

## 2. THE GLOBAL NORMALIZATION ALGORITHM

In this section, we review the global version of the normalization algorithm. To begin with, we fix our notation and give some general facts on normalization. For this,  $A$  may be any reduced Noetherian ring. We write

$$\text{Spec}(A) = \{P \subset A \mid P \text{ prime ideal}\}$$

for the *spectrum* of  $A$ . The *vanishing locus* of an ideal  $J$  of  $A$  in  $\text{Spec}(A)$  is the set  $V(J) = \{P \in \text{Spec}(A) \mid P \supset J\}$ . We denote by

$$N(A) = \{P \in \text{Spec}(A) \mid A_P \text{ is not normal}\}$$

the *non-normal locus* of  $A$ , and by

$$\text{Sing}(A) = \{P \in \text{Spec}(A) \mid A_P \text{ is not regular}\}$$

the *singular locus* of  $A$ . Then  $N(A) \subset \text{Sing}(A)$ , with equality holding if  $A$  is the coordinate ring of a curve (see [9, Theorem 4.4.9]).

**Definition 2.1.** The *conductor* of  $A$  is

$$\mathcal{C}_A = \text{Ann}_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subset A\}.$$

Note that  $\mathcal{C}_A$  is the largest ideal of  $A$  which is also an ideal of  $\overline{A}$ .

To emphasize the role of the conductor, we note:

**Lemma 2.2.** *Let  $A$  be a reduced Noetherian ring. Then  $N(A) \subset V(\mathcal{C}_A)$ . Furthermore,  $\overline{A}$  is a finite  $A$ -module iff  $\mathcal{C}_A$  contains a non-zero-divisor of  $A$ . In this case,  $N(A) = V(\mathcal{C}_A)$ .*

Note, however, that the conductor can only be computed a posteriori when  $\overline{A}$  is already known.

**Definition 2.3.** Let  $A$  be a reduced Noetherian ring. A *test ideal* for  $A$  is a radical ideal  $J \subset A$  such that  $V(\mathcal{C}_A) \subset V(J)$ . A *test pair* for  $A$  consists of a test ideal  $J$  together with a non-zero-divisor  $g \in J$  of  $A$ .

Test pairs appear in the Grauert and Remmert normality criterion which is fundamental to algorithmic normalization (see [15], [17, Prop. 3.6.5]). The normalization algorithm of de Jong (see [8], [10]) and its improvement, the algorithm of Greuel et al. [16], are based on this criterion. Both algorithms apply to any reduced affine algebra  $A = K[X_1, \dots, X_n]/I$  over a perfect field  $K$ . By means of primary decomposition, we may reduce to the case where  $A$  is equidimensional. In this case, since we work over a perfect field, the Jacobian ideal<sup>1</sup>  $M$  of  $A$  is non-zero and contained

<sup>1</sup>The *Jacobian ideal*  $M$  of  $A = K[X_1, \dots, X_n]/I$  is generated by the images of the  $c \times c$  minors of the Jacobian matrix  $(\frac{\partial f_i}{\partial X_j})$ , where  $c$  is the codimension, and  $f_1, \dots, f_r$  are generators for  $I$ . By the Jacobian criterion,  $V(M) = \text{Sing}(A)$  (see [13, Theorem 16.19]).

in the conductor  $\mathcal{C}_A$ , so that we may choose the radical  $J = \sqrt{M}$  together with any non-zero divisor  $g$  in  $J$  as a test pair (see [16, Lemma 4.1]). The idea of finding  $\bar{A}$  is then to successively enlarge  $A$  by finite ring extensions  $A_{i+1} \cong \text{Hom}_{A_i}(J_i, J_i) \cong \frac{1}{g}(gJ_i :_{A_i} J_i) \subset \bar{A} \subset \mathbb{Q}(A)$ , with  $A_0 = A$  and  $J_i = \sqrt{JA_i}$ , until the normality criterion of Grauert and Remmert allows us to stop. As already pointed out in Remark 1.3, the algorithm of Greuel et al. is designed so that it returns an ideal  $U \subset A$  together with an element  $d \in A$  such that  $\bar{A} = \frac{1}{d}U \subset \mathbb{Q}(A)$ .

**Remark 2.4.** If  $M$  is non-zero and contained in  $\mathcal{C}_A$ , then any non-zero divisor in  $M$  is valid as a denominator: If  $0 \neq c \in M$ , and  $\bar{A} = \frac{1}{d}U$  as above, then  $c \cdot \frac{1}{d}U =: U'$  is an ideal of  $A$ , and  $\frac{1}{d}U = \frac{1}{c}U'$ .

**Example 2.5.** Let  $A$  be the coordinate ring of the curve  $C$  with defining polynomial  $f(X, Y) = X^5 - Y^2(Y - 1)^3 \in \mathbb{Q}[X, Y]$ . Then

$$J := \langle x, y(y - 1) \rangle_A$$

is the radical of the Jacobian ideal, so we can take  $(J, x)$  as a test pair. In its first step, the normalization algorithm yields

$$A_1 = \frac{1}{x}U_1 = \frac{1}{x} \langle x, y(y - 1)^2 \rangle_A.$$

In the next steps, we get

$$A_2 = \frac{1}{x^2}U_2 = \frac{1}{x^2} \langle x^2, xy(y - 1), y(y - 1)^2 \rangle_A$$

and

$$A_3 = \frac{1}{x^3}U_3 = \frac{1}{x^3} \langle x^3, x^2y(y - 1), xy(y - 1)^2, y^2(y - 1)^2 \rangle_A.$$

In the final step, we find that  $A_3$  is normal and, hence, equal to  $\bar{A}$ .

### 3. NORMALIZATION OF CURVES VIA LOCALIZATION

In this section, we discuss the local to global variant of the normalization algorithm proposed by Böhm et al. [5]. To simplify our presentation, we focus on the case of a reduced Noetherian ring with a finite singular locus (which includes our case of interest here). Our starting point is Proposition 3.1 below which is also fundamental to our new algorithm. In formulating the proposition, if  $P \in \text{Spec}(A)$  and  $A \subset A' \subset \bar{A}$  is an intermediate ring, we write  $A'_P$  for the localization of  $A'$  at  $A \setminus P \subset A'$ .

**Proposition 3.1.** *Let  $A$  be a reduced Noetherian ring with a finite singular locus  $\text{Sing}(A) = \{P_1, \dots, P_s\}$ . For  $i = 1, \dots, s$ , let an intermediate ring  $A \subset A^{(i)} \subset \bar{A}$  be given such that  $A_{P_i}^{(i)} = \bar{A}_{P_i}$ . Then*

$$\sum_{i=1}^s A^{(i)} = \bar{A}.$$

*Proof.* A more general result is proved in [5, Proposition 3.2]. □

**Definition 3.2.** We call any ring  $A^{(i)}$  as in the proposition a *local contribution* to  $\bar{A}$  at  $P_i$ . If in addition  $A_{P_j}^{(i)} = A_{P_j}$  for  $j \neq i$ , we speak of a *minimal local contribution* to  $\bar{A}$  at  $P_i$ .

**Remark 3.3.** Note that such a contribution is uniquely determined since, by definition, its localization at each  $P \in \text{Spec}(A)$  is determined.

Given a reduced affine algebra  $A$  over a perfect field  $K$  with a finite singular locus, Proposition 3.1 allows us to split the computation of  $\bar{A}$  into local tasks at the primes  $P_i \in \text{Sing}(A)$ . One way of finding the minimal local contributions  $A^{(i)}$  is to apply the local version of the normalization algorithm from [5] which relies on a local variant of the Grauert and Remmert criterion. For each  $i$ , the basic idea is to use  $P_i$  together with a suitable element  $g_i$  of the Jacobian ideal instead of a test pair as in Definition 2.3.

**Example 3.4.** As in Example 2.5, let  $A$  be the coordinate ring of the curve  $C$  with defining polynomial  $f(X, Y) = X^5 - Y^2(Y - 1)^3 \in \mathbb{Q}[X, Y]$ . Note that  $C$  has a double point of type  $A_4$  at  $(0, 0)$  and a triple point of type  $E_8$  at  $(0, 1)$ . If we apply the strategy above, taking  $P_1 = \langle x, y \rangle_A$ ,  $P_2 = \langle y - 1, x \rangle_A$  and  $g_1 = g_2 = x$ , we get local contributions  $\frac{1}{d_i}U_i$ ,  $i = 1, 2$ . Specifically,

$$\begin{aligned} d_1 &= x^2 \quad \text{and} \quad U_1 = \langle x^2, y(y - 1)^3 \rangle_A, \\ d_2 &= x^3 \quad \text{and} \quad U_2 = \langle x^3, x^2 y^2 (y - 1), y^2 (y - 1)^2 \rangle_A. \end{aligned}$$

Summing up the local contributions, we get  $\bar{A} = \frac{1}{d}U$  with  $d = x^3$  and

$$U = \langle x^3, y(y - 1)^3 x, y^2 (y - 1)^2 x^2, y^2 (y - 1)^2 \rangle_A.$$

Note that  $U$  coincides with the ideal  $U_3$  computed in Example 2.5.

**Remark 3.5.** In Example 3.4, the normalization of the local ring  $A_{P_2}$  is  $\overline{A_{P_2}} = \frac{1}{x^3} \langle x^3, x^2(y - 1), (y - 1)^2 \rangle_{A_{P_2}}$ . Indeed, since  $y^2$  is a unit in  $\overline{A_{P_2}}$ , this follows by localizing  $U_2$  at  $P_2$ . Note, however, that  $(y - 1)/x$  and  $(y - 1)^2/x^3$  are not integral over  $A$ . Hence,  $\frac{1}{x^3} \langle x^3, x^2(y - 1), (y - 1)^2 \rangle_A$  is not a local contribution to  $A$  at  $P_2$ .

Relying on the Jacobian criterion, we may find the primes in  $\text{Sing}(A)$  by means of primary decomposition. If there is precisely one such prime, this requires (possibly expensive) computations which are only needed to detect this fact. In the case of a plane curve  $C$  considered here, supposing that one singularity  $P$  of  $C$  is already known to us, we may check whether  $P$  is the only singularity of  $C$  by comparing the local Tjurina number of  $C$  at  $P$  with the total Tjurina number of  $C$ . Computing the total Tjurina number via Gröbner bases over the rationals, however, can be expensive due to coefficient swell. To overcome this problem, we provide an efficient modular criterion. Note that though singularities at infinity do not matter for obtaining integral bases, the criterion takes these singularities into account. That is, it is formulated in the projective setting.

Let  $K$  be any field, let  $F \in K[X, Y, Z]$  be a square-free homogeneous polynomial of positive degree, and let  $\Gamma = \text{Proj}(K[X, Y, Z]/\langle F \rangle)$  be the projective curve defined by  $F$ . Moreover, write

$$S = K[X, Y, Z]/\langle F_X, F_Y, F_Z \rangle,$$

where  $F_X, F_Y, F_Z$  are the partial derivatives of  $F$ . Then, taking Euler's rule into account,  $\Gamma_{\text{sing}} = \text{Proj}(S) \subset \Gamma$  is the singular locus of  $\Gamma$ . For any  $Q \in \Gamma_{\text{sing}}$ , let  $S_{(Q)}$  be the homogeneous localization of  $S$  at  $Q$ . Then

$$\tau_Q(\Gamma) = \dim_K S_{(Q)}$$

is the Tjurina number of  $\Gamma$  at  $Q$ . For example, if  $P = \langle X, Y \rangle$ , then

$$\tau_P(\Gamma) = \dim_K (K[X, Y]_{\langle X, Y \rangle} / \langle f, f_X, f_Y \rangle),$$

with  $f = F(X, Y, 1)$ . The Tjurina number of  $\Gamma$  in the chart  $X \neq 0$  is

$$\tau_{X \neq 0}(\Gamma) = \dim_K (K[X, Y] / \langle f, f_X, f_Y \rangle),$$

and similarly for the other coordinate charts. Finally,

$$\tau(\Gamma) = \deg \text{Proj}(S) = \sum_{Q \in \Gamma_{\text{sing}}} \tau_Q$$

is the total Tjurina number of  $\Gamma$ .

**Proposition 3.6.** Let  $F \in \mathbb{Q}[X, Y, Z]$  be a square-free homogeneous polynomial of positive degree with integer coefficients. Let  $q$  be a prime number such that the reduction  $F_q$  of  $F$  modulo  $q$  is non-zero. Consider the curves  $\Gamma = \text{Proj}(\mathbb{Q}[X, Y, Z]/\langle F \rangle)$  and  $\Gamma_q = \text{Proj}(\mathbb{F}_q[X, Y, Z]/\langle F_q \rangle)$ , and let  $P = \langle X, Y \rangle$ . Suppose that

$$\tau_P(\Gamma_q) = \tau_P(\Gamma) > 0 \quad \text{and} \quad \tau_{X \neq 0}(\Gamma_q) = \tau_{Y \neq 0}(\Gamma_q) = 0.$$

Then  $\Gamma_{\text{sing}} = \{P\}$ .

*Proof.* By [2, Theorem 5.3], considering the Hilbert functions of

$$S = \mathbb{Q}[X, Y, Z] / \langle F_X, F_Y, F_Z \rangle \text{ and } \\ S_q = \mathbb{F}_q[X, Y, Z] / \langle (F_X)_q, (F_Y)_q, (F_Z)_q \rangle,$$

we have

$$\text{HF}_S(t) \leq \text{HF}_{S_q}(t), \text{ for all } t.$$

Since the Tjurina numbers are the leading coefficients of the respective Hilbert polynomials, this implies that

$$\tau(\Gamma) \leq \tau(\Gamma_q).$$

On the other hand, if  $\tau_{X \neq 0}(\Gamma_q) = \tau_{Y \neq 0}(\Gamma_q) = 0$ , then  $(\Gamma_q)_{\text{sing}} = \{P\}$ , so that

$$\tau(\Gamma_q) = \tau_P(\Gamma_q) = \tau_P(\Gamma) \leq \tau(\Gamma).$$

Combining both inequalities yields

$$\tau_P(\Gamma) = \tau(\Gamma)$$

and, thus,  $\Gamma_{\text{sing}} = \{P\}$ . □

**Remark 3.7.** The invariants in the criterion can be obtained efficiently by a standard basis computation over  $\mathbb{Q}$  with respect to a local ordering and by standard basis computations over  $\mathbb{F}_p$  with respect to a global and a local ordering, respectively.

#### 4. PUISEUX SERIES AND INTEGRALITY

We discuss some basic facts about Puiseux series and their connection to integrality.

**4.1. Puiseux Series.** Let  $K \subset L$  be a field extension, with  $L$  algebraically closed. The *field of Puiseux series* over  $L$  is the field

$$L\{\{X\}\} = \bigcup_{m=1}^{\infty} L((X^{1/m})).$$

The Newton-Puiseux theorem, which is closely related to the aforementioned finiteness theorem of Emmy Noether, says that  $L\{\{X\}\}$  is the algebraic closure of  $L((X))$ . In particular,  $L[[X^{1/m}]]$  is the integral closure of  $L[[X]]$  in  $L((X^{1/m}))$ . See [13, Chapter 13], [1, Lecture 12].

We have a canonical *valuation map*

$$v : L\{\{X\}\} \setminus \{0\} \rightarrow \mathbb{Q}, \gamma \mapsto v(\gamma),$$

where  $v(\gamma)$  is the smallest exponent appearing in a term of  $\gamma$ . By convention,  $v(0) = \infty$ . The corresponding *valuation ring*  $L\{\{X\}\}_{v \geq 0}$  consists of all Puiseux series with non-negative exponents only. Henceforth it will be denoted by  $\mathcal{P}_X$ .

If  $p \in L\{\{X\}\}[Y]$  is any polynomial in  $Y$  with coefficients in  $L\{\{X\}\}$ , the *valuation* of  $p$  at  $\gamma \in L\{\{X\}\}$  is defined to be  $v_\gamma(p) := v(p(x, \gamma))$ .

**4.2. Conjugate Puiseux Series.** Two Puiseux series in  $L\{\{X\}\}$  are called *conjugate* if they are conjugate as field elements over  $K((X))$ .

**4.3. Rational Part.** Let  $\gamma = a_1 X^{t_1} + a_2 X^{t_2} + \dots + a_k X^{t_k} + a_{k+1} X^{t_{k+1}} + \dots \in \mathcal{P}_X$ , with  $0 \leq t_1 < t_2 < \dots$ . Let  $k \geq 0$  be such that  $a_i X^{t_i} \in K[X]$  for  $1 \leq i \leq k$  and  $a_{k+1} X^{t_{k+1}} \notin K[X]$ . Then we call  $a_1 X^{t_1} + \dots + a_k X^{t_k}$  the *rational part* of  $\gamma$ , and  $a_{k+1} X^{t_{k+1}}$  its *first non-rational term*.



**4.4. Characteristic Exponents.** For  $\gamma \in \mathcal{P}_X$ , let  $m \in \mathbb{N}$  be minimal with  $\gamma \in L[[X^{1/m}]]$ , and write  $\gamma = \sum_{i \geq 0} b_i X^{i/m}$ , with coefficients  $b_i \in L$ . If  $m = 1$ , there are no characteristic exponents. If  $m \geq 2$ , the *characteristic exponents* of  $\gamma$  are defined inductively by

$$\begin{aligned} e_1 &:= \min\{i \mid b_i \neq 0 \text{ and } m \nmid i\}, \\ e_\nu &:= \min\{i \mid b_i \neq 0, \gcd(e_1, \dots, e_{\nu-1}) \nmid i\} \text{ for } \nu > 1. \end{aligned}$$

Then  $e_1 < e_2 < \dots$ . In fact, there are only finitely many  $e_\nu$ , and these are coprime.

**Example 4.1.** If  $\gamma = 2X^{1/2} + X^{3/4} + 6X^{5/4} - 5X^{17/8}$ , the common denominator is  $m = 8$ . Writing  $\gamma = 2X^{4/8} + X^{6/8} + 6X^{10/8} - 5X^{17/8}$ , we see that the characteristic exponents are  $e_1 = 4$ ,  $e_2 = 6$ , and  $e_3 = 17$ .

**4.5. Puiseux Expansions.** In what follows, we consider a monic polynomial  $g \in K[[X]][Y]$  of degree  $m$  in  $Y$ . By the Newton-Puiseux theorem,  $g$  has  $m$  roots  $\gamma_1, \dots, \gamma_m \in L\{\{X\}\}$ :

$$g = (Y - \gamma_1) \cdots (Y - \gamma_m) \in K[[X]][Y].$$

The monic assumption guarantees that each root  $\gamma_i$  is, in particular, integral over  $L[[X]]$  and, thus, contained in some  $L[[X^{1/m}]] \subset \mathcal{P}_X$ . That is, the terms of  $\gamma_i$  have non-negative exponents only.

The roots  $\gamma_i$  are called the *Puiseux expansions* of  $g$  (at  $X = 0$ ).

**4.6. The Newton-Puiseux Algorithm.** The Puiseux expansions of  $g$  can be computed recursively up to any given order using the Newton-Puiseux algorithm (see, for example, [9]). Essentially, to get a solution  $a_1 X^{t_1} + a_2 X^{t_2} + \dots$  of  $g(X, \gamma(X)) = 0$ , with  $t_1 < t_2 < \dots$ , the algorithm proceeds as follows: Starting from  $g^{(0)} = g$  and  $K^{(0)} = K((X))$ , we commence the  $i$ th step of the algorithm by looking at a polynomial  $g^{(i-1)} \in K^{(i-1)}[Y]$ . We then choose one face  $\Delta$  of the Newton polygon of  $g^{(i-1)}$  such that all the other points of the polygon lie on or above the line containing the face. Let  $g_\Delta^{(i-1)}$  be the sum of terms of  $g^{(i-1)}$  involving the monomials of  $g^{(i-1)}$  on  $\Delta$ . That is, if  $-\frac{w_1}{w_2}$  is the slope of  $\Delta$ , then  $g_\Delta^{(i-1)}$  is the sum of terms of  $g^{(i-1)}$  of lowest  $(1, \frac{w_2}{w_1})$ -weighted degree. We write  $d_i$  for this degree. Choose an irreducible factor of  $g_\Delta^{(i-1)}$  over  $K^{(i-1)}$  and a root  $q_i$  of that factor. Note that  $q_i$  is of type  $q_i = c_i X^{\frac{w_2}{w_1}}$ , where  $c_i$  is a root of the polynomial  $g_\Delta^{(i-1)}(1, Y)$ . Now, let  $K^{(i)} = K^{(i-1)}(q_i)$  and set  $g^{(i)} = \frac{1}{X^{d_i}} g^{(i-1)}(X, q_i \cdot (1 + Y))$ . Then the  $i$ -th term of the expansion to be constructed is  $a_i X^{t_i} = q_1 \cdots q_i$ . It is clear from this construction that different conjugacy classes of expansions arise from different choices for the faces and irreducible factors of  $g_\Delta^{(i-1)}$  over  $K^{(i-1)}$ , respectively.

**Example 4.2.** The eight Puiseux expansions of the polynomial

$$\begin{aligned} g = & Y^8 + (-4X^3 + 4X^5)Y^7 + (4X^3 - 4X^5 - 10X^6)Y^6 + (4X^5 - 6X^6)Y^5 \\ & + (6X^6 - 8X^8)Y^4 + (8X^8 - 4X^9)Y^3 + (4X^9 + 4X^{10})Y^2 + 4X^{11}Y + X^{12} \in \mathbb{Q}[X, Y] \end{aligned}$$

are conjugate over  $\mathbb{Q}((X))$ ; their singular parts are of type

$$q_1 + q_1 q_2 + q_1 q_2 q_3,$$

where the  $q_i$  satisfy

$$q_1^2 + X^3 = 0, \quad q_2^2 + \frac{1}{2X} q_1 = 0, \quad \text{and} \quad q_3^2 + \frac{1}{16X} q_1 = 0.$$

To see this, note that the Newton polygon of  $g^{(0)} = g$  has only one face  $\Delta_0$ , leading to  $g_{\Delta_0}^{(0)} = (X^3 + Y^2)^4$  and the extension

$$K_0 = \mathbb{Q}((X)) \subset K_1 = K_0[iX^{\frac{3}{2}}].$$

In the next step,  $g^{(1)}$  has only one face  $\Delta_1$ , yielding

$$g_{\Delta_1}^{(1)} = 4 \left( 2Y^2 + \frac{q_1}{X} \right)^2$$

and

$$K_1 \subset K_2 = K_0[iX^{\frac{3}{2}}, (1-i)X^{\frac{1}{4}}].$$

Finally, also  $g^{(2)}$  has only one face  $\Delta_2$ , which corresponds to

$$g_{\Delta_2}^{(2)} = -2 \cdot \left(8Y^2 - \frac{q_1}{X}\right)$$

and the extension

$$K_2 \subset K_3 = K_0[iX^{\frac{3}{2}}, (1-i)X^{\frac{1}{4}}, (1+i)X^{\frac{1}{4}}] = K_0[i, X^{\frac{1}{4}}].$$

**4.7. Regularity Index and Singular Part.** If  $\gamma = a_1X^{t_1} + a_2X^{t_2} + \dots$  is a Puiseux expansion of  $g$ , with  $0 \leq t_1 < t_2 < \dots$  and no  $a_i$  zero, we define the *regularity index* of  $\gamma$  (with respect to  $g$ ) to be the least exponent  $t_k$  such that no other Puiseux expansion of  $g$  has the same initial part  $a_1X^{t_1} + \dots + a_kX^{t_k}$ . This initial part is, then, called the *singular part* of  $\gamma$  (with respect to  $g$ ).

**4.8. Maximal Integrality Exponents.** Let  $\Gamma = \{\gamma_1, \dots, \gamma_m\}$  be the set of Puiseux expansions of  $g$ . The *valuation* of  $p \in L\{\{X\}\}[Y]$  at  $g$  is defined to be  $v_g(p) = \min_{1 \leq i \leq m} v_{\gamma_i}(p)$ . Note that if  $p$  is monic of degree  $d$  in  $Y$ , where  $1 \leq d \leq m-1$ , and

$$p = (Y - \eta_1(X)) \cdots (Y - \eta_d(X))$$

is the factorization of  $p$  in  $L\{\{X\}\}[Y]$ , then

$$v_g(p) = \min_{1 \leq i \leq m} \sum_{j=1}^d v(\gamma_i - \eta_j).$$

**Lemma 4.3.** Let  $g \in K[[X]][Y]$  be monic of degree  $m$  in  $Y$ , with Puiseux expansions  $\gamma_1, \dots, \gamma_m$ . Fix an integer  $d$  with  $1 \leq d \leq m-1$ . If  $\mathcal{A} \subset \{1, \dots, m\}$  is a subset of cardinality  $d$ , set

$$\text{Int}(\mathcal{A}) = \min_{i \notin \mathcal{A}} \left( \sum_{j \in \mathcal{A}} v(\gamma_i - \gamma_j) \right).$$

Choose a subset  $\tilde{\mathcal{A}} \subset \{1, \dots, m\}$  of cardinality  $d$  such that  $\text{Int}(\tilde{\mathcal{A}})$  is maximal among all  $\text{Int}(\mathcal{A})$  as above, and set  $\tilde{p} = \prod_{j \in \tilde{\mathcal{A}}} (Y - \gamma_j) \in \mathcal{P}_X[Y]$ . Then  $v_g(\tilde{p}) = \text{Int}(\tilde{\mathcal{A}})$ , and this number is the maximal valuation  $v_g(q)$ , for  $q \in L\{\{X\}\}[Y]$  monic of degree  $d$  in  $Y$ .

*Proof.* That  $v_g(\tilde{p}) = \text{Int}(\tilde{\mathcal{A}})$  is clear from the definitions. That this number is the maximum valuation  $v_g(q)$  as claimed follows as in the proof of [21, Theorem 5.1], where the case  $d = m-1$  is treated.  $\square$

In the situation of the lemma, with  $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ , we write

$$o(\Gamma, d) = v_g(\tilde{p}).$$

Then

$$o(\Gamma, 1) \leq \dots \leq o(\Gamma, m-1)$$

by construction.

In case  $d = m-1$ , we abbreviate

$$\text{Int}_i = \text{Int}(\{1, \dots, i-1, i+1, \dots, m\}) = \sum_{j \neq i} v(\gamma_i - \gamma_j).$$

**Example 4.4.** Let  $g = (Y^2 + 2X^3) + Y^3 \in \mathbb{Q}[X, Y]$ . The Puiseux expansions of  $g$  are

$$\gamma_1 = a_1X^{3/2} + X^3 + \dots,$$

$$\gamma_2 = a_2X^{3/2} + X^3 + \dots,$$

$$\gamma_3 = -1 - 2X^3 + \dots,$$



where  $a_1, a_2$  are the roots of  $X^2 + 2$ . Then  $\text{Int}_1 = 3/2 + 0 = 3/2$ ,  $\text{Int}_2 = 3/2 + 0 = 3/2$ , and  $\text{Int}_3 = 0 + 0 = 0$ , so that both  $i = 1$  and  $i = 2$  maximize the valuation. Taking  $i = 1$ , we get  $\tilde{p} = (Y - \gamma_2)(Y - \gamma_3)$  and  $o(\Gamma, 2) = 3/2$ .

**Example 4.5.** Let  $g = (Y^3 + X^2)(Y^2 - X^3) + Y^6 \in \mathbb{Q}[X, Y]$ . The Puiseux expansions of  $g$  are

$$\begin{aligned} \gamma_1 &= a_1 X^{2/3} + \dots, & \gamma_4 &= X^{3/2} + \dots, \\ \gamma_2 &= a_2 X^{2/3} + \dots, & \gamma_5 &= -X^{3/2} + \dots, \\ \gamma_3 &= a_3 X^{2/3} + \dots, & \gamma_6 &= 1 + \dots, \end{aligned}$$

where the  $a_i$  are the roots of  $X^3 + 1 = 0$ . Then  $\text{Int}_1 = \text{Int}_2 = \text{Int}_3 = 2/3 + 2/3 + 2/3 + 2/3 + 0 = 8/3$ ,  $\text{Int}_4 = \text{Int}_5 = 3/2 + 2/3 + 2/3 + 2/3 + 0 = 7/2$ , and  $\text{Int}_6 = 0$ . We conclude that  $o(\Gamma, 5) = 7/2$ .

Note that for  $R$  any one of the rings  $K[X]$ ,  $K[[X]]$ ,  $K((X))$  or  $\mathcal{P}_X$ , we have  $R[Y] \subset L\{\{X\}\}[Y]$ , hence the definition of  $v_g(p)$  also applies for  $p \in R[Y]$ .

**Lemma 4.6.** *Let  $g \in K[[X]][Y] \subset L\{\{X\}\}[Y]$  be monic of degree  $m$  in  $Y$ , let  $1 \leq d \leq m - 1$ , and let  $R$  be one of the rings  $K[X]$ ,  $K[[X]]$ ,  $K((X))$ ,  $\mathcal{P}_X$ , or  $L\{\{X\}\}$ . The maximal valuation  $v_g(q)$ ,  $q \in R[Y]$  monic of degree  $d$  in  $Y$ , is independent of the choice of  $R$  from among this list.*

*Proof.* By Lemma 4.3, there is a polynomial  $\tilde{p} = \prod_{j \in \tilde{\mathcal{A}}} (Y - \gamma_j)$  with  $|\tilde{\mathcal{A}}| = d$  which maximizes the valuation in case  $R = L\{\{X\}\}$ , but is contained in  $\mathcal{P}_X[Y]$ . Choose an integer  $m$  such that  $\tilde{p} \in L((X^{1/m}))[Y]$ . By truncating the coefficients of  $\gamma_j$  to degree  $v_g(\tilde{p})$ , we get a polynomial  $\bar{p} \in L(X^{1/m})[Y]$ . In fact, for the field  $\tilde{K} \subset L$  obtained by adjoining the coefficients of  $\bar{p}$  to  $K$ , we have  $\bar{p} \in \tilde{K}[X^{1/m}][Y]$ . Since  $\bar{p}$  is monic in  $Y$ , by applying the trace map of  $\tilde{K}(X^{1/m})$  over  $K(X)$  to  $\bar{p}$  and dividing by the integer lead coefficient of the resulting polynomial, we get a monic polynomial  $0 \neq p \in K[X][Y]$  of degree  $d$ . By construction,  $p$  satisfies  $v_g(p) \geq v_g(\tilde{p})$ . Note that  $K[X]$  is included in all the rings  $R$  in the above list, hence the reverse inequalities are trivial, and the result follows.  $\square$

**Remark 4.7.** With notation as above, note that for any representative in  $K((X))[Y]$  of an element of  $K[X]_{\langle X \rangle}[Y]$ , the valuation at  $g$  is the same. Hence we can also define  $v_g(p)$  for  $p \in K[X]_{\langle X \rangle}[Y]$  and the maximal valuation  $v_g(q)$  with  $q \in K[X]_{\langle X \rangle}[Y]$ , is the same as the maximal valuation with  $q \in K[X][Y]$ , for monic polynomials of the same degree.

The reason for considering the valuations  $v_g(p)$  is that they are directly related to integrality. Suppose

$$A = K[x, y] = K[X, Y]/\langle f \rangle$$

is the coordinate ring of an irreducible plane curve  $C$  of degree  $n$  with assumptions and notation as in the introduction.

**Definition 4.8.** Let  $R = K[X]$ ,  $K[X]_{\langle X \rangle}$  or  $K[[X]]$  and  $B = R[Y]/\langle f \rangle$ . If  $q \in R[Y]$  is monic in  $Y$  of degree  $1 \leq i \leq n - 1$ , and  $e$  is the maximal integer such that  $\frac{q(x, y)}{x^e}$  is integral over  $B$ , we call  $e_R(q) := e$  the *integrality exponent of  $q$  with respect to  $f$  and  $R$* .

**Lemma 4.9.** *Let  $p \in K[X]_{\langle X \rangle}[Y]$  be monic in  $Y$  of degree  $1 \leq i \leq n - 1$ . Then*

$$e_{K[X]_{\langle X \rangle}}(p) = \lfloor v_f(p) \rfloor.$$

*Proof.* By [19, Theorem 3.2.6],  $p(x, y)/x^e$  is integral over  $K[X]_{\langle X \rangle}[Y]/\langle f \rangle$  iff  $v_\gamma(p/X^e) \geq 0$  for every Puiseux expansion  $\gamma$  of  $f$ . Since  $v_f(p)$  is defined to be the minimum of the respective  $v_\gamma(p)$ , the result follows.  $\square$

**Lemma 4.10.** *Let  $p \in K[[X]][Y]$  be monic in  $Y$  of degree  $1 \leq i \leq n - 1$ . Then*

$$e_{K[[X]]}(p) = \lfloor v_f(p) \rfloor.$$

*Proof.* Again, by [19, Theorem 3.2.6],  $p(x, y)/x^e$  is integral over  $K[[X]][Y]/\langle f \rangle$  iff  $v_\gamma(p/X^e) \geq 0$  for every Puiseux expansion  $\gamma$  of  $f$ .  $\square$

**Lemma 4.11.** *Let  $p \in K[X, Y]$  be monic in  $Y$  of degree  $1 \leq i \leq n - 1$ . Then*

$$e_{K[X]}(p) = \lfloor v_f(p) \rfloor.$$

*Proof.* We have to show that  $p(x, y)/x^e$  is integral over  $A$  iff  $v_\gamma(p/X^e) \geq 0$  for every Puiseux expansion  $\gamma$  of  $f$  (see also [21, Section 2.4]). If  $p(x, y)/x^e$  is integral over  $A$ , then also over  $K[X]_{\langle X \rangle}[Y]/\langle f \rangle$ , hence  $v_\gamma(p/X^e) \geq 0$  for every Puiseux expansion  $\gamma$  of  $f$ . For the converse, note that  $v_\gamma(p/X^e) \geq 0$  for all Puiseux expansions  $\gamma$  of  $f$  at  $x \neq 0$ . Hence,  $p(x, y)/x^e \in \overline{A}$  by [19, Theorem 3.2.6].  $\square$

**Definition 4.12.** For  $q \in K[X]_{\langle X \rangle}[Y]$  or  $q \in K[[X]][Y]$ , we define

$$e(q) = \lfloor v_f(q) \rfloor.$$

Note that, by Lemmata 4.9, 4.10 and 4.11, we have  $e(q) = e_R(q)$  as long as  $q$  or a representative of  $q$  is in  $R[Y]$ .

**Definition 4.13.** Let  $0 \leq i < n$  be an integer. Taking Lemma 4.6 into account, the number

$$e_i := \max \{ e_R(q) \mid q \in R[Y] \text{ monic in } Y, \deg q = i \}$$

is independent of the choice of  $R$  among  $K[X]$ ,  $K[X]_{\langle X \rangle}$  and  $K[[X]]$ . We call  $e_i$  the *maximal integrality exponent with respect to  $f$  in degree  $i$* .

**Definition 4.14.** We call

$$E(f) = e_{n-1} = \lfloor o(\Gamma, n - 1) \rfloor$$

the *maximal integrality exponent of  $f$* .

## 5. NORMALIZATION OF PLANE CURVES VIA LOCALIZATION AND COMPLETION: DECOMPOSING INTO BRANCHES

From now on,

$$A = K[C] = K[x, y] = K[X, Y]/\langle f(X, Y) \rangle$$

will be the coordinate ring of an irreducible plane curve  $C$  with assumptions as in the introduction. In particular,  $f$  is assumed to be monic in  $Y$ . We focus on the case where  $P = \langle X, Y \rangle \in \text{Sing}(A)$ . Applying the Weierstrass preparation theorem, we get a unique factorization

$$(1) \quad f = f_0 f_1 \cdots f_r,$$

where  $f_0 \in K[[X]][Y]$  is a unit in  $K[[X, Y]]$  and  $f_1, \dots, f_r$  are irreducible Weierstrass polynomials in  $K[[X]][Y]$  (see, for example, [9]). We write

$$m_i = \deg_Y(f_i), \quad i = 0, \dots, r$$

and refer to  $f_1, \dots, f_r$  as the *branches* of  $f$  at  $P$ .

In this section, we will study first integral bases for the branches of the singularity  $P$  from a theoretical point of view and explain how these can be combined to give an integral basis for  $K[[X]][Y]/\langle f_1 \cdots f_r \rangle$ .

In what follows, we consider a monic polynomial  $g \in K[[X]][Y]$  of degree  $m$  in  $Y$  and write

$$B = K[[X]][Y]/\langle g \rangle.$$

(We do not assume  $g$  to be a Weierstrass polynomial, although in this section we apply the results to that case.) By abuse of notation,  $x, y$  will also denote the residue classes of  $X, Y$  modulo  $g$ . Applying [19, Theorem 3.3.4] to the PID

$$K[[x]] \subset K((x)) \subset K((x))[y]$$

we see that  $\overline{B}$  is a free  $K[[x]]$ -module of rank  $m$ .

**Remark 5.1.** In particular,  $K[[X]][Y]/\langle f_1 \cdots f_r \rangle$  and its normalization are a free  $K[[x]]$ -modules of rank  $m_1 + \cdots + m_r$ .

**Definition 5.2.** With notation as above, we refer to any integral basis of  $\overline{B}$  over  $K[[x]]$  as an *integral basis* for  $g$ .

**Lemma 5.3.** *With notation as above, there exist polynomials  $p_i \in K[X][Y]$ ,  $0 \leq i \leq m-1$  of degree  $i$  in  $Y$  with leading coefficients  $x^{t_i}$ ,  $t_i \in \mathbb{Z}_{\geq 0}$ , and  $e_i \in \mathbb{Z}_{\geq 0}$ ,  $1 \leq i \leq m-1$ , such that*

$$\mathcal{B} = \left\{ 1 = p_0, \frac{p_1(x, y)}{x^{e_1+t_1}}, \dots, \frac{p_{m-1}(x, y)}{x^{e_{m-1}+t_{m-1}}} \right\}$$

*is an integral basis for  $g$ . Furthermore, if  $q \in K[[X]][Y]$  is any polynomial of degree  $1 \leq k \leq m-1$  in  $Y$  with leading coefficient  $x^t$ , and  $e$  is an integer such that  $\frac{q(x, y)}{x^{e+t}}$  is integral over  $K[[x]]$ , then  $e \leq e_k$ . In particular, the  $e_i$  depend only on  $g$  and satisfy  $0 = e_0 \leq e_1 \leq \cdots \leq e_{m-1}$ .*

*Proof.* Each square matrix with entries in  $K[[x]]$  of maximal rank has a uniquely determined upper triangular Hermite normal form  $(p_{ij})$ , where the diagonal elements are of type  $p_{ii} = x^{\nu_i}$ , and where the  $p_{ij}$ ,  $j > i$ , are polynomials in  $K[x]$  of degree  $< \nu_i$  (see [12]). Hence, given any integral basis for  $g$  where the denominators are powers of  $x$ , we can first reduce the numerators modulo the monic polynomial  $g$  to get elements of  $Y$ -degree at most  $m-1$ . Then taking the largest power of  $x$  in the denominators as common denominator, we construct the matrix of coefficients of the numerators and apply unimodular row operations as in Remark 1.2 to get after cancellation an integral basis  $1 = b_0, b_1, \dots, b_{m-1}$ , where each  $b_i$  is of the form  $\frac{p_i(x, y)}{x^{t_i+e_i}}$ , with  $e_i, t_i \in \mathbb{Z}_{\geq 0}$  ( $t_i \leq \nu_i$ ),  $p_i \in K[X][Y]$  polynomial of degree  $i$  in  $Y$  with leading coefficient  $x^{t_i}$ . This shows the first statement of the lemma. The second statement and, thus, the uniqueness result follows by expressing  $\frac{q(x, y)}{x^{e+t}}$  as a  $K[[x]]$ -linear combination of the  $b_i$ ,  $0 \leq i \leq k$ . To see that  $e_{i-1} \leq e_i$ , for each  $i$ , consider  $q = Y \cdot p_{i-1}$ .  $\square$

**Remark 5.4.** We refer to [12] for the computational aspects of the lemma up to any desired precision (that is, up to which power in  $X$  the coefficients are developed). We note that in our case, since the starting point is an integral basis, we know that  $1, y, \dots, y^{m-1}$  can be expressed as  $K[[X]]$ -linear combinations of the elements in the basis, hence the exponent of the common denominator of the input basis gives an a-priori bound for the maximum precision needed.

**Remark 5.5.** We will show after the next proposition that, in fact, any integral basis in the shape of the lemma is guaranteed to have monic numerators, that is  $t_i = 0$  for  $0 \leq i \leq m-1$ .

In Section 7.5, we will present a practical method for finding integral bases as in Lemma 5.3. The starting point for this is the following proposition.

**Proposition 5.6.** *With notation as above, for  $1 \leq i \leq m-1$ , let monic polynomials  $p_i \in K[[X]][Y]$  of degree  $i$  in  $Y$  be given, and let  $e_i$  be the maximal integrality exponent with respect to  $g$  in degree  $i$ . Then*

$$1 = p_0, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_{m-1}(x, y)}{x^{e(p_{m-1})}}$$

*is an integral basis for  $g$  iff  $e(p_i) = e_i$  for  $1 \leq i \leq m-1$ .*

*Proof.* If the given elements form an integral basis for  $g$ , then necessarily  $e(p_i) \leq e_i$  for each  $i$ . Suppose that  $e(p_i) < e_i$  for some  $i$ , and choose an element  $q \in K[[X]][Y]$  which is monic in  $Y$  of degree  $i$  and satisfies  $e(q) = e_i$ . Then  $\frac{q}{x^{e_i}} \in \left\langle 1, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_{m-1}(x, y)}{x^{e(p_{m-1})}} \right\rangle_{K[[x]]}$ , which is impossible since the exponent of each denominator on the right hand side is smaller than  $e_i$  by the third part of Lemma 5.3.

For the converse, suppose that  $e(p_i) = e_i$  for each  $i$ . Set  $B' = \left\langle 1, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_{m-1}(x, y)}{x^{e(p_{m-1})}} \right\rangle_{K[[x]]}$ . Then  $B \subset B' \subset \overline{B}$ , and we have to show that  $B' = \overline{B}$ . That is, given a polynomial  $q \in K[[X]][Y]$

of degree  $0 \leq i \leq m-1$  in  $Y$  such that  $\frac{q(x,y)}{x^e} \in \overline{B}$  for some integer  $e \geq 0$ , we have to show that  $\frac{q(x,y)}{x^e} \in B'_i$ , where  $B'_i = \left\langle 1, \frac{p_1(x,y)}{x^{e(p_1)}}, \dots, \frac{p_i(x,y)}{x^{e(p_i)}} \right\rangle_{K[[X]]}$ .

We do induction on  $i$ . There is nothing to show in case  $i = 0$ . If  $i \geq 1$ , let  $c$  be the leading coefficient of  $q \in K[[X]][Y]$ . We can assume that  $c = x^t$ ,  $t \in \mathbb{Z}_{\geq 0}$ , since any other factor is invertible in  $K[[X]]$ . Write  $q$  as a product  $q = x^t \tilde{q}$ , with  $\tilde{q} \in K((X))[Y]$  monic in  $Y$ . By Lemma 4.6 and the definition of  $p_i$  we have  $v_g(\tilde{q}) \leq e(p_i)$ , hence

$$e \leq e(q) \leq t + v_g(\tilde{q}) \leq t + e(p_i) = e(x^t p_i).$$

This implies that  $\frac{x^t p_i(x,y)}{x^e} \in \overline{B}$  and hence it is in  $B'_i$ . Since  $\deg_Y(q - x^t p_i) < i$  and  $\frac{q(x,y)}{x^e} - \frac{x^t p_i(x,y)}{x^e} \in \overline{B}$ , by the induction hypothesis, we get  $\frac{q(x,y)}{x^e} - \frac{x^t p_i(x,y)}{x^e} \in B'_{i-1} \subset B'_i$ . Therefore  $\frac{q(x,y)}{x^e} \in B'_i$  as claimed.  $\square$

**Remark 5.7.** Together with Lemma 4.6, the last proposition proves the existence of an integral basis  $\left\{1 = p_0, \frac{p_1(x,y)}{x^{e(p_1)}}, \dots, \frac{p_{m-1}(x,y)}{x^{e(p_{m-1})}}\right\}$  where the  $p_i \in K[X][Y]$  are monic of degree  $i$  in  $Y$ ,  $0 \leq i \leq m-1$ .

**Proposition 5.8.** *With notation as above, if  $\left\{1 = p_0, \frac{p_1(x,y)}{x^{e_1+t_1}}, \dots, \frac{p_{m-1}(x,y)}{x^{e_{m-1}+t_{m-1}}}\right\}$  is any integral basis of  $g$  in the shape of Lemma 5.3, the polynomials  $p_i$  in the integral basis are monic in  $Y$ .*

*Proof.* Suppose for  $p_k$  we have  $t_k > 0$ . Since no cancellation is possible, there must be some coefficient of  $p_k$  that is not multiple of  $x$ . We now take an integral basis  $\mathcal{B}$  for  $g$  as in the last remark, and call  $\mathcal{B}_k$  the elements in  $\mathcal{B}$  of degree at most  $k$ . We can express  $p_k/x^{e_k+t_k}$  as a  $K[[X]]$ -linear combination of the elements in  $\mathcal{B}_k$  (no elements in  $\mathcal{B}$  of larger degree can be used). But the largest power of  $x$  in the denominators of  $\mathcal{B}_k$  is  $e_k$ , hence we get a contradiction.  $\square$

We now return to the branches  $f_1, \dots, f_r$  at  $P$  of our given polynomial  $f$  and apply the above to the product  $g = f_1 \cdots f_r$ .

**Proposition 5.9** (Splitting of Normalization). *Let  $f_1, \dots, f_r$  be the branches of  $f$  at  $P$  as in Equation (1). For each  $i$ , set  $h_i = \prod_{j=1, j \neq i}^r f_j$ . Then the  $f_i$  and  $h_i$  are coprime in  $K((X))[Y]$ , so that there are elements  $a_i, b_i \in K[[X]][Y]$  and integers  $c_i \in \mathbb{N}$  such that*

$$a_i f_i + b_i h_i = X^{c_i}, \quad \text{for } i = 1, \dots, r.$$

Furthermore, the normalization of  $K[[X]][Y]/\langle f_1 \cdots f_r \rangle$  splits as

$$\overline{K[[X]][Y]/\langle f_1 \cdots f_r \rangle} \cong \bigoplus_{i=1}^r \overline{K[[X]][Y]/\langle f_i \rangle},$$

and the splitting is given by

$$(t_1 \bmod f_1, \dots, t_r \bmod f_r) \mapsto \sum_{i=1}^r \frac{b_i h_i t_i}{X^{c_i}} \bmod f_1 \cdots f_r.$$

*Proof.* Clear by the Chinese remainder theorem and its proof. See [9, Theorem 1.5.20].  $\square$

Given an integral basis for each branch, we can make the splitting of normalization explicit:

**Corollary 5.10.** *With notation as in Proposition 5.9, for  $i = 1, \dots, r$ , let*

$$1 = p_0^{(i)}, \frac{p_1^{(i)}}{X^{e_1^{(i)}}}, \dots, \frac{p_{m_i-1}^{(i)}}{X^{e_{m_i-1}^{(i)}}}$$

represent an integral basis as in Lemma 5.3 for  $f_i$ , and set

$$\mathcal{B}^{(i)} = \left\{ \frac{b_i h_i}{X^{c_i}}, \frac{b_i h_i p_1^{(i)}}{X^{c_i+e_1^{(i)}}}, \dots, \frac{b_i h_i p_{m_i-1}^{(i)}}{X^{c_i+e_{m_i-1}^{(i)}}} \right\}$$

or each  $i$ . Then  $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$  is an integral basis for  $f_1 \cdots f_r$ .

*Proof.* Immediate from Proposition 5.9.  $\square$

Finally, we note that we can apply the construction in Lemma 5.3 to the elements in  $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$  to get an integral basis in the shape

$$1 = p_0, \frac{p_1(x, y)}{x^{e_1}}, \dots, \frac{p_{m-1}(x, y)}{x^{e_{m-1}}},$$

with polynomials  $p_i \in K[X][Y]$  of degree  $i$  in  $Y$  and non-negative integers  $e_i$ ,  $1 \leq i \leq m-1$ , where the polynomials  $p_i$  are monic by Proposition 5.8.

Using some of the tools developed in the subsequent sections, we illustrate the corollary by an example:

**Example 5.11.** Let  $f = (Y^3 + X^2)(Y^2 - X^3) + Y^6$  be as in Example 4.5 and let  $A = K[X, Y]/\langle f \rangle = K[x, y]$ . In  $K[[X]][Y]$ ,  $f$  can be factorized as  $f = f_0 f_1 f_2$ , whose developments up to degree 3 in  $X$  are  $f_0 \equiv Y + (-X^3 - X^2 + 1)$ ,  $f_1 \equiv Y^3 + (X^3 + X^2)Y^2 + (-X^2)Y + X^2$  and  $f_2 \equiv Y^2 - X^3$ .

Following Proposition 5.9, applying the extended GCD algorithm to  $f_1$  and  $h_1 = f_2$  we get the coefficients  $a_1$  and  $b_1$  whose developments up to degree 3 in  $X$  are  $a_1 \equiv -4X^3Y - 2X^3 - 2X^2Y - X^2 + XY - Y - 1$  and  $b_1 \equiv -4X^3Y^2 - 2X^3Y - 2X^2Y^2 - 3X^3 - 2X^2Y + XY^2 - Y^2 - Y$  satisfying  $a_1 f_1 + b_1 h_1 = X^2$ , with  $h_1 = f_2$ .

The rings  $K[[X]][Y]/\langle f_i \rangle$ ,  $i = 1, 2$ , have integral bases  $\left\{1, y, \frac{y^2}{x}\right\}$  and  $\left\{1, \frac{y}{x}\right\}$ . By Corollary 5.10, an integral basis for the normalization of  $K[[X]][Y]/\langle f_1 f_2 \rangle$  is given by  $\mathcal{B}^{(1)} \cup \mathcal{B}^{(2)}$ , where

$$\mathcal{B}^{(1)} = \left\{ \frac{b_1 f_2}{x^2}, \frac{b_1 f_2 y}{x^2}, \frac{b_1 f_2 y^2}{x^3} \right\} \quad \text{and} \quad \mathcal{B}^{(2)} = \left\{ \frac{a_1 f_1}{x^2}, \frac{a_1 f_1 y}{x^3} \right\}.$$

We can now apply the construction from Lemma 5.3. Since the maximum power of  $x$  appearing in the denominators of  $\mathcal{B}^{(1)} \cup \mathcal{B}^{(2)}$  is  $X^3$ , we can truncate all the coefficients appearing in the computation to degree 3 in  $x$ . We obtain the integral basis

$$\left\{ 1, y, \frac{y^2}{x}, \frac{y^3}{x^2}, \frac{y^4 + x^2 y}{x^3} \right\}$$

for the normalization of  $K[[X]][Y]/\langle f_1 f_2 \rangle$ .

Note that in this example, the maximum power of  $X$  appearing in the denominators was not known a priori, but in a practical algorithm it is required for computing the developments of the factors  $f_1$ ,  $f_2$  and the coefficients  $a_1$ ,  $b_1$ . We address this problem in Proposition 7.10.

## 6. NORMALIZATION OF PLANE CURVES VIA LOCALIZATION AND COMPLETION: LOCAL CONTRIBUTIONS

In this section, we will keep the notation and assumptions of the previous section. For simplicity, we will assume that the origin is the only singularity at  $X = 0$ , which can always be achieved by a linear coordinate change. Alternatively, it is easy to extend our algorithms for the case of the presence of more than one singularity at  $X = 0$ .

Using Puiseux series, we will show how to pass from an integral basis for the normalization of  $K[[X]][Y]/\langle f_1 \cdots f_m \rangle$  as in Corollary 5.10 to an integral basis for the normalization of  $K[[X]][Y]/\langle f \rangle$ . If the elements of that basis are polynomials, we will show that this is already an integral basis for the normalization of  $K[X]_{\langle X \rangle}[Y]/\langle f \rangle$ . Moreover, since we are assuming that the origin is the only singularity at  $X = 0$ , it will also be an integral basis for the local contribution to the normalization at  $P = \langle X, Y \rangle$ .

**Proposition 6.1.** *Let  $f = f_0 g$  be a factorization of  $f$  with  $f_0, g \in K[[X]][Y]$ ,  $f_0$  a unit in  $K[[X]][Y]$  and  $g$  a Weierstrass polynomial, let  $A = K[[X]][Y]/\langle f \rangle$  and  $P = \langle X, Y \rangle$ . Write*

$n = \deg_Y f$ ,  $d_0 = \deg_Y f_0$  and  $m = \deg_Y g$ . Suppose that  $P$  is the only singularity of  $f$  at  $X = 0$ . Let

$$1 = p_0, \frac{p_1}{x^{e_1}}, \dots, \frac{p_{m-1}}{x^{e_{m-1}}}$$

be an integral basis for  $K[[X]][Y]/\langle g \rangle$  with polynomials  $p_i \in K[X][Y]$  monic in  $Y$  of degree  $i$ . Let  $\bar{f}_0 \in K[X][Y]$  be a (monic) polynomial with

$$\bar{f}_0 \equiv f_0 \pmod{X^{e_{m-1}}}.$$

Then

$$1, y, y^2, \dots, y^{d_0-1}, \bar{f}_0 p_0, \frac{\bar{f}_0 p_1}{x^{e_1}}, \dots, \frac{\bar{f}_0 p_{m-1}}{x^{e_{m-1}}}$$

is an integral basis for the normalization of  $K[[X]][Y]/\langle f \rangle$ .

*Proof.* We first show that the elements  $\bar{f}_0 p_i / x^{e_i}$ ,  $1 \leq i \leq m-1$ , are integral over  $A$ . Suppose that  $\gamma$  is a Puiseux expansion of  $f$ . If  $\gamma(0) = 0$  then  $v_\gamma(\bar{f}_0 p_i) \geq v_\gamma(p_i) \geq v_g(p_i) \geq e_i$ . If  $\gamma(0) \neq 0$  then  $v_\gamma(\bar{f}_0 p_i) \geq v_\gamma(\bar{f}_0) \geq e_{m-1} \geq e_i$  by definition of  $\bar{f}_0$ .

To apply Proposition 5.6, we have to show for  $i = 0, \dots, m-1$  that  $e_i$  is maximal among all  $e(q)$  where  $q \in K[[X]][Y]$  monic in  $Y$  of  $\deg_Y(q) = i + d_0$ , and that  $e(q) = 0$  for all  $q \in K[[X]][Y]$  with  $\deg_Y(q) < d_0$ . Suppose  $q(x, y)/x^e$ ,  $e > 0$  is integral over  $A$  where  $q \in K[[X]][Y]$  is monic in  $Y$  of degree  $s < \deg_Y(f)$ . Let

$$q = q_0 h$$

be a factorization of  $q$  with  $q_0, h \in K[[X]][Y]$ ,  $q_0(0, 0)$  not 0 and  $h$  a Weierstrass polynomial. Write  $\eta_1, \dots, \eta_s$  for the Puiseux expansions of  $q$ .

The assumption that the origin is the only singularity at  $X = 0$  implies that all the Puiseux expansions of  $f_0$  have pairwise different non-zero constant term. Suppose that  $\gamma^{(1)}, \dots, \gamma^{(d_0)}$  are the Puiseux expansions of  $f_0$  and  $\gamma^{(d_0+1)}, \dots, \gamma^{(n)}$  are the expansions of  $g$ . Then  $\gamma^{(i)} = a_0^{(i)} + a_1^{(i)} x^{t_2^{(i)}} + \dots$ ,  $1 \leq i \leq d_0$ , with  $a_0^{(i)} \neq 0$  for all  $1 \leq i \leq d_0$  and  $a_0^{(i)} \neq a_0^{(j)}$  for  $1 \leq i < j \leq d_0$ . Moreover,  $\gamma^{(i)} = a_1^{(i)} x^{t_2^{(i)}} + \dots$  for  $i > d_0$ . Assume that for some  $1 \leq i \leq d_0$  there is no expansion  $\eta_j$ ,  $1 \leq j \leq s$ , with initial term  $a_0^{(i)}$ . Then

$$v_f(q) = \min_{1 \leq i \leq n} v_{\gamma^{(i)}}(q) = \min_{1 \leq i \leq n} \sum_{j=1}^s v(\gamma_i - \eta_j) = 0,$$

which contradicts the hypotheses.

Hence, for  $s < d_0$  the maximal integrality exponent is 0. Moreover, if  $s \geq d_0$  then all  $a_0^{(i)}$  for  $1 \leq i \leq d_0$  have to appear as initial terms of some  $\eta_j$ ,  $1 \leq j \leq s$ , and they are pairwise different. So we can assume that for each  $1 \leq i \leq d_0$  the initial term of  $\eta_i$  is  $a_0^{(i)}$ . Then  $q_0 = (y - \eta_1) \cdot \dots \cdot (y - \eta_{d_0}) \cdot u$  where  $u \in \mathcal{P}_X[Y]$ , in particular

$$d_0 \leq \deg_Y(q_0).$$

For any Puiseux expansion  $\gamma^{(i)}$  of  $f$  we have

$$v_{\gamma^{(i)}}(q) = v_{\gamma^{(i)}}(q_0) + v_{\gamma^{(i)}}(h) = \begin{cases} v_{\gamma^{(i)}}(h) & \text{if } \gamma^{(i)}(0) = 0 \\ v_{\gamma^{(i)}}(q_0) & \text{if } \gamma^{(i)}(0) \neq 0, \end{cases}$$

hence

$$\begin{aligned} v_f(q) &= \min_{1 \leq i \leq n} v_{\gamma^{(i)}}(q) = \min \left\{ \min_{1 \leq i \leq d_0} v_{\gamma^{(i)}}(q_0), \min_{d_0 < i \leq n} v_{\gamma^{(i)}}(h) \right\} \\ &= \min\{v_{f_0}(q_0), v_g(h)\} \leq v_g(h). \end{aligned}$$

This implies that

$$e \leq \lfloor v_f(q) \rfloor \leq \lfloor v_g(h) \rfloor \leq e_{s-\deg_Y(q_0)}.$$

For the last inequality, we use that  $e_{s-\deg_Y(q_0)}$  is maximal among all  $\lfloor v_g(p) \rfloor$  with  $p \in K[[X]][Y]$ . Since  $d_0 \leq \deg_Y(q_0)$ , we have

$$e \leq e_{s-\deg_Y(q_0)} \leq e_{s-d_0},$$



which proves our claim.  $\square$

**Remark 6.2.** For the last proposition, we do not use the assumption  $p_i \in K[X][Y]$ ,  $0 \leq i \leq m-1$ , and we do not need to truncate  $f_0$ . However, by doing this we obtain an integral basis with numerators in  $K[X][Y]$ , which is then, by faithfully flatness, also an integral basis for the normalization of  $K[X]_{\langle X \rangle}[Y]/\langle f \rangle$ . Moreover, if  $P = \langle X, Y \rangle$  is the only singularity at  $X = 0$ , it is also a  $K[X]$ -basis for the local contribution to the normalization of  $K[X, Y]/\langle f \rangle$  at the origin, as we show next.

We need first the following version of Lemma 5.6.

**Lemma 6.3.** *Let  $f \in K[X, Y]$  monic of  $Y$ -degree  $n$ . Let  $p_1, \dots, p_{n-1} \in K[X, Y]$  be polynomials which are monic in  $Y$  of degree  $i$  such that for all  $1 \leq i \leq n-1$ ,  $e(p_i)$  is the maximal integrality exponent with respect to  $f$  in degree  $i$ . Then*

$$1 = p_0, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_{n-1}(x, y)}{x^{e(p_{n-1})}}$$

*form a  $K[x]$ -module basis of a local contribution to the normalization at any prime  $Q$  with  $\langle x \rangle \subset Q$ . If  $P = \langle X, Y \rangle$  is the only singularity at  $X = 0$ , then it is a  $K[X]$ -module basis for the minimal local contribution at  $P$ .*

*Proof.* Suppose that  $e(p_i)$  is the maximal integrality exponent with respect to  $f$  in degree  $i$ . By Corollary 4.6

$$e(p_i) \geq v_f(p)$$

for all  $p \in K((X))[Y]$  of degree  $i$ .

Denote by  $A'$  the  $K[x]$ -module generated by  $1, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_{n-1}(x, y)}{x^{e(p_{n-1})}}$ . By assumption,  $A' \subset \overline{A}$ . We prove that  $A'$  is the minimal local contribution at  $P$ .

First, given a polynomial  $q(X, Y) \in K[X, Y]$  of degree  $0 \leq i \leq n-1$  in  $Y$  such that  $\frac{q(x, y)}{x^e} \in \overline{A}$  for some integer  $e \geq 0$ , we show that  $\frac{q(x, y)}{x^e} \in A'_i$ , where  $A'_i = \left\langle 1, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_i(x, y)}{x^{e(p_i)}} \right\rangle_{K[x]}$ , as we did in the proof of Lemma 5.6.

We do induction on  $i$ , the claim being trivial for  $i = 0$ . For  $i \geq 1$ , dividing  $q$  by the lead coefficient with respect to  $Y$  write  $q(X, Y) = c(X)q'(X, Y)$  with  $c(X) \in K[X]$  and  $q'(X, Y) \in K((X))[Y]$ , monic in  $Y$ . By the above remark and the definition of  $p_i$  we have  $v_f(q') \leq e(p_i)$ , hence

$$e \leq e(q) \leq e(c) + v_f(q') \leq e(c) + e(p_i) = e(cp_i).$$

(Here the last equality holds, since  $c(X)$  has integer valuation and only depends on  $X$ ). This implies that  $\frac{c(x)p_i(x, y)}{x^e} \in \overline{A}$ . Moreover, writing  $c'(x) = \frac{c(x)}{x^{e(c)}}$  we obtain that

$$\frac{c(x)p_i(x, y)}{x^e} = c'(x) \frac{p_i(x, y)}{x^{e-e(c)}} \in A'_i.$$

Since  $\deg_Y(q - cp_i) < i$  and  $\frac{q(x, y)}{x^e} - \frac{c(x)p_i(x, y)}{x^e} \in \overline{A}$ , by the induction hypothesis, we get

$$\frac{q(x, y)}{x^e} - \frac{c(x)p_i(x, y)}{x^e} \in A'_{i-1} \subset A'_i.$$

Hence,  $\frac{q(x, y)}{x^e} \in A'_i$  as claimed.

We now pass to the localization. For

$$D = K[X]_{\langle X \rangle}[Y]/\langle f \rangle \text{ and } D' = \left\langle 1, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_{n-1}(x, y)}{x^{e(p_{n-1})}} \right\rangle_{K[x]_{\langle x \rangle}}$$

we have  $D \subset D' \subset \overline{D}$ . Let  $\frac{q(x, y)}{d(x)} \in \overline{D}$  be an arbitrary element of  $\overline{D}$  with polynomials  $q \in K[X, Y]$  and  $d \in K[X]$ . Write  $d(x) = x^e \cdot d'(x)$  with a unit  $d'(x) \in K[x]_{\langle x \rangle}$ . Then also  $\frac{q(x, y)}{x^e} \in \overline{D}$ , hence there exists an  $h(X) \in K[X]$  such that  $h(x) \in K[x]_{\langle x \rangle}$  is a unit and  $h(x) \frac{q(x, y)}{x^e} \in \overline{A}$ . By the above argument,  $h(x) \frac{q(x, y)}{x^e} \in A' \subset D'$ , so  $\frac{q(x, y)}{d(x)} \in D'$ , hence,  $D' = \overline{D}$ .



To localize  $A'$  at primes of  $A$ , we first prove that  $A'$  is a commutative ring with 1. This amounts to show that  $A'$  is closed under multiplication. Any product of elements can be written as

$$\frac{q(x, y)}{x^e} \cdot \frac{q'(x, y)}{x^{e'}} = \frac{q''(x, y)}{x^{e+e'}}$$

with  $q'' \in K[X, Y]$  and  $\deg_Y(q'') < n$ . Since the product is in  $\overline{A}$ , by the above argument, the product is in  $A'$ . Since  $A'$  is a ring it is also an  $A$ -module.

We have

$$A'_Q = \overline{D}_Q = \overline{D_Q} = \overline{A_Q}$$

for all  $Q \in \text{Spec } A$  with  $\langle x \rangle \subset Q$ . Moreover,  $A'_Q = A_Q$  for all  $Q$  with  $\langle x \rangle \not\subset Q$ , since the denominators of the generators of  $A'$  are in  $\langle x \rangle$ . If  $P = \langle X, Y \rangle$  is the only singularity at  $X = 0$ , then  $\overline{A_Q} = A_Q$  for all  $Q \in \text{Spec } A$  with  $\langle x \rangle \subset Q$ ,  $Q \neq P$ , hence it is a minimal contribution.  $\square$

**Corollary 6.4.** *Let*

$$\mathcal{B} = \left\{ 1 = p_0, \frac{p_1(x, y)}{x^{e(p_1)}}, \dots, \frac{p_{n-1}(x, y)}{x^{e(p_{n-1})}} \right\}$$

*be an integral basis for  $K[[X]][Y]/\langle f \rangle$ , where  $p_i$  are polynomials. Then it is also an integral basis for the normalization of  $K[X]_{\langle X \rangle}[Y]/\langle f \rangle$  and a  $K[X]$ -module basis for the local contribution at any prime  $Q$  with  $\langle x \rangle \subset Q$ . If  $P = \langle X, Y \rangle$  is the only singularity at  $X = 0$ , then it is a  $K[X]$ -module basis for the minimal local contribution at  $P$ .*

*Proof.* Clear by the previous lemma and Lemma 4.6.  $\square$

## 7. NORMALIZATION OF PLANE CURVES VIA LOCALIZATION AND COMPLETION: THE ALGORITHMIC POINT OF VIEW

Let  $A = K[x, y] = K[X, Y]/\langle f(X, Y) \rangle$  be as before. In this section, we show how to compute a local contribution to  $\overline{A}$  at each prime ideal  $P \in \text{Sing}(A)$  via Puiseux expansions, Hensel's lemma, and Proposition 5.9. The normalization  $\overline{A}$  itself and an integral basis for  $\overline{A}$  over  $K[x]$ , respectively, are then obtained along the lines of Proposition 3.1 and Remark 1.3.

We start with a sketch of the algorithm.

**7.1. Summary of the Algorithm.** From a **theoretical point of view**, the algorithm involves the following steps:

- (1) If the prime ideal  $P \in \text{Sing}(A)$  corresponds to a (single)  $K$ -rational singularity, **translate the singularity to the origin**. If  $P$  corresponds to a set of conjugate singularities over  $K$ , extend the base field  $K$  as needed, and **translate one of the singularities to the origin**. In any case, apply a linear transformation so that the translated singularity is the only singularity at  $X = 0$ .

For the singularity at the origin, do (to simplify the presentation, we will still write  $f$  for the transformed equation of our curve):

- (2) Determine the **maximum integrality exponent**  $E(f)$  as described in Section 4.8.
- (3) Determine integers  $c_i$ ,  $1 \leq i \leq r$ , as in Proposition 5.9 and the **factorization**  $f = \prod_{i=0}^r f_i$  of  $f$  into branches, developing each  $f_i$  up to degree  $E(f) + c_i$  in  $X$ . Here, make use of Hensel's lemma as described in Sections 7.3 and 7.4.
- (4) Compute the Bézout coefficients  $b_i$ ,  $1 \leq i \leq r$ , from Proposition 5.9 up to order  $E(f) + c_i$ .
- (5) For each branch  $f_i$ ,  $1 \leq i \leq r$ , use the algorithm from Section 7.5 to compute **integral bases for the branches**  $K[[X]][Y]/\langle f_i \rangle$  as in Lemma 5.3 up to order  $E(f) + c_i$  in  $X$ .
- (6) Construct the generating sets  $\mathcal{B}^{(i)}$ ,  $1 \leq i \leq r$ , as in Corollary 5.10, and apply the construction in Lemma 5.3 to compute an integral basis for  $K[[X]][Y]/\langle f_1 \cdots f_r \rangle$  with numerators in  $K[X, Y]$ .
- (7) Compute an integral basis for  $K[[X]][Y]/\langle f \rangle$  using Algorithm 10, which is based on Proposition 6.1. Since the numerators in the output are elements in  $K[X][Y]$ , by Corollary 6.4, this is the local contribution to the normalization of  $A$  at the origin.

- (8) Apply the **inverse translation** to the elements of the local contribution to restore the singularity to the original position.
- (9) If  $P$  corresponds to a set of conjugate singularities, then use Remark 7.17 to modify the numerators and denominators of the local contribution in order to obtain the **local contribution to  $\bar{A}$  at  $P$**  over the original field.

From a **practical point of view**, we face the problem that, in the approach outlined above, we need to determine the  $c_i$  *a priori*. Moreover, the computation of the Bézout coefficients  $b_i$  via the extended Euclidean algorithm is very time consuming. To remedy these issues, relying on Proposition 7.10 below, we will replace the  $b_i$  and  $c_i$  in Steps 4 and 3 by easier to construct polynomials  $\beta_i \in K[X, Y]$  and appropriate vanishing orders, respectively.

We refer to the following sections for more details.

**7.2. Puiseux Expansions.** The factors  $f_i$  appearing in the decomposition

$$f = f_0 g = f_0 f_1 \cdots f_r$$

of  $f$  into its branches and a unit  $f_0$  as in Equation (1) in Section 5 correspond to complete sets of conjugate Puiseux expansions. Developed up to a given degree, the  $f_i$  may hence be found by computing the expansions and their respective products. Since this is computationally involved, we propose a different approach which, via Hensel's lemma, makes considerably less use of the Newton-Puiseux algorithm. In describing the new approach, we use the notation below.

We partition the set of all Puiseux expansions of  $f$  into *Puiseux blocks*. A Puiseux block represented by an expansion  $\gamma$  with  $\gamma(0) = 0$  is obtained by collecting all expansions whose rational part agrees with that of  $\gamma$  and whose first non-rational term is conjugate to that of  $\gamma$  over  $K((X))$ . A *Puiseux segment* is defined as the union of all blocks having the same initial exponent. That is, we have one Puiseux segment for each face of the Newton polygon of  $f$ . In addition, all Puiseux expansions  $\gamma$  of  $f$  with  $\gamma(0) \neq 0$  are grouped together to a single Puiseux block of an extra Puiseux segment. In this way, the Puiseux expansions of  $f$  are divided into Puiseux segments, each segment consists of Puiseux blocks, and each block is the union of classes of conjugate expansions.

**Example 7.1.** Suppose that the Puiseux expansions of the given polynomial  $f$  are

$$\begin{aligned} \gamma_1 &= 1 + X^2 + \dots, & \gamma_6 &= X + b_1 X^{5/2} + X^3 + \dots, \\ \gamma_2 &= -1 + 3X + \dots, & \gamma_7 &= X + b_2 X^{5/2} + X^3 + \dots, \\ \gamma_3 &= a_1 X^{3/2} + 2X^2 + \dots, & \gamma_8 &= X + b_1 X^{5/2} + X^4 + \dots, \\ \gamma_4 &= a_2 X^{3/2} + 2X^2 + \dots, & \gamma_9 &= X + b_2 X^{5/2} + X^4 + \dots, \\ \gamma_5 &= X + 3X^2 + \dots, \end{aligned}$$

where  $\{\gamma_3, \gamma_4\}$ ,  $\{\gamma_6, \gamma_7\}$  and  $\{\gamma_8, \gamma_9\}$  are pairs of conjugate Puiseux series. Then  $\{\gamma_1, \gamma_2\}$  is the segment of expansions  $\gamma$  with  $\gamma(0) \neq 0$ . Another segment is  $\{\gamma_3, \gamma_4\}$  (which consists of one block containing a single class of conjugate expansions). All the other expansions form a single segment, consisting of the blocks  $\{\gamma_5\}$  and  $\{\gamma_6, \gamma_7, \gamma_8, \gamma_9\}$ . The last block contains two classes of conjugate expansions, namely  $\{\gamma_6, \gamma_7\}$  and  $\{\gamma_8, \gamma_9\}$ .

**7.3. Hensel's Lemma.** We begin by recalling the statement of the lemma:

**Lemma 7.2.** *Let  $F \in K[[X]][Y]$  be a monic polynomial in  $Y$ , and assume that  $F(0, Y) = g_0 h_0$ , with monic polynomials  $g_0, h_0 \in K[Y]$  such that  $\langle g_0, h_0 \rangle = K[Y]$ . Then there exist unique monic polynomials  $G, H \in K[[X]][Y]$  such that*

- (1)  $F = GH$ ,
- (2)  $G(0, Y) = g_0$ ,  $H(0, Y) = h_0$ .

*In fact, for each  $m \in \mathbb{N}$ , there exist unique  $g_m, h_m \in K[X, Y]$  of  $X$ -degree  $\leq m$  such that*

- (3)  $F \equiv g_m h_m$  in  $(K[[X]]/\langle X^{m+1} \rangle)[Y]$ ,

$$(4) \quad g_m \equiv g_i, \quad h_m \equiv h_i \text{ in } (K[[X]]/\langle X^{i+1} \rangle)[Y], \quad i = 0, \dots, m-1.$$

*Proof.* See, for example, [1]. □

Conditions (3) and (4) imply that the polynomials  $g_m$  and  $h_m$  can be computed inductively along the  $X$ -degree, solving for each  $m$  a system of  $n$  linear equations in  $n$  variables, where  $n$  is the  $Y$ -degree of  $F$ : For each  $0 \leq i \leq n-1$ , we get an equation by comparing the coefficients of  $X^m Y^i$  in  $F$  and in  $g_m h_m$ . For further reference in this paper, we state the resulting procedure as Algorithm 1, omitting the actual computation steps.

---

**Algorithm 1** HenselLift

---

**Input:**  $F \in K[X, Y]$  monic in  $Y$ ;  $g_0, h_0 \in K[Y]$  monic with  $F(0, Y) = g_0 h_0$ ,  $\langle g_0, h_0 \rangle = K[Y]$ ;  $d \in \mathbb{N}$ .  
**Output:**  $g, h \in K[X, Y]$  of  $X$ -degree  $\leq d$ , with  $g(0, Y) = g_0$ ,  $h(0, Y) = h_0$ , and  $F \equiv gh \pmod{X^{d+1}}$ .

---

When applying **HenselLift** as indicated in Section 7.2, we first address the Puiseux segment consisting of all Puiseux expansions  $\gamma$  of  $f$  with  $\gamma(0) \neq 0$ . That is, we decompose  $f$  as  $f = f_0 g$  as in (1), separating the unit  $f_0$  from the component  $g$  vanishing at the origin (we develop  $f_0$  and  $g$  up to a certain order). This is summarized in Algorithm 2.

---

**Algorithm 2** SeparateUnit

---

**Input:**  $f \in K[X, Y]$  irreducible and monic in  $Y$ , with  $f(0, 0) = 0$ ;  $d \in \mathbb{N}$ .  
**Output:**  $f_0, g \in K[[X]][Y]$  as in Equation (1), developed up to  $X$ -degree  $d$ .  
 1: compute monic  $g_0, h_0 \in K[Y]$  with  $h_0 = Y^k$  for some  $k \in \mathbb{N}_{\geq 1}$ ,  $Y \nmid g_0$ , and  $f(0, Y) = g_0 h_0$   
 2: **return** **HenselLift**( $f, g_0, h_0, d$ )

---

**Example 7.3.** Let  $f = (Y - X)(Y + X)(Y + 2X) + Y^7$ . Then there are three Puiseux expansions satisfying  $\gamma(0) = 0$  and four expansions with  $\gamma(0) \neq 0$  (note that  $f(0, Y) = Y^3 + Y^7 = Y^3(1 + Y^4)$ ). We write  $\gamma_1, \dots, \gamma_4$  for the latter expansions and  $\gamma_5 = X + \dots, \gamma_6 = -X + \dots, \gamma_7 = -2X + \dots$  for the expansions vanishing at the origin. We apply **SeparateUnit** to develop the products  $f_0 = \gamma_1 \cdots \gamma_4$  and  $g = \gamma_5 \gamma_6 \gamma_7$  up to degree 2. It calls **HenselLift**( $f, g_0, h_0, 2$ ) with  $g_0 = 1 + Y^4$  and  $h_0 = Y^3$ . The output is  $g_2 = 5X^2 Y^2 - 2XY^3 + Y^4 + 1$  and  $h_2 = Y^3 + 2XY^2 - 2X^2 Y$ .

Alternatively, we could compute  $f = f_0 g$  by means of the Weierstrass Division Theorem. However, the use of Hensel's Lemma allows for more generality since it does not require to have one factor vanishing at the origin. This will be useful for our local version of Hensel's Lemma. It is also useful when the singularity has no  $K$ -rational coordinates, as we can modify our algorithms to avoid moving the singularity to the origin, which requires the use of an algebraic extensions. (For keeping the presentation clear, we do not give the details of this strategy.)

**7.4. A Local Version of Hensel's Lemma.** Having computed the decomposition  $f = f_0 g$  as in the previous section, our next goal is to separate the different Puiseux segments corresponding to  $g$ . Here, we cannot apply Hensel's lemma directly since all factors of  $g$  vanish at the origin, so no matter how we choose  $g_0, h_0$ , the condition  $\langle g_0, h_0 \rangle = K[Y]$  will not be satisfied (consider, for example, the product  $(Y - \gamma_1)(Y - \gamma_2)(Y - \gamma_3)$  in Example 4.5).

To overcome this problem, we transform  $g$  as explained in what follows. Write

$$\begin{aligned} \gamma_1 &= a_1^1 X^{t_1^1} + a_2^1 X^{t_2^1} + \dots, \\ \gamma_2 &= a_1^2 X^{t_1^2} + a_2^2 X^{t_2^2} + \dots, \\ &\vdots \\ \gamma_s &= a_1^s X^{t_1^s} + a_2^s X^{t_2^s} + \dots \end{aligned}$$

for the Puiseux expansions of  $g$ , and suppose for simplicity that  $t := t_1^1 = \min_{1 \leq i \leq s} t_1^i$ . Naively, we are now tempted to substitute  $X^t Y$  for  $Y$  in  $g = (Y - \gamma_1) \cdots (Y - \gamma_s) \in K[[X]][Y]$  and cancel out  $X^t$  in all factors in order to separate the Puiseux segment corresponding to  $t$  from the rest. However, since this would introduce fractional exponents and thus force us to leave  $K[[X]][Y]$ , we proceed in a slightly different way: Write  $t = u/v$ , with  $u, v \in \mathbb{N}_{\geq 1}$ , and substitute  $X^v$  for  $X$  and  $X^u Y$  for  $Y$ . Then set

$$\begin{aligned} F(X, Y) &= g(X^v, X^u Y) / X^{su} \\ &= (Y - (a_1^1 + a_2^1 X^{\tilde{t}_1^1} + \dots)) \cdots (Y - (a_1^s X^{\tilde{t}_1^s} + \dots)) \in K[[X]][Y]. \end{aligned}$$

Now,  $F$  has factors not vanishing at the origin, and these correspond to the Puiseux expansions of  $f$  forming the Puiseux segment with smallest initial exponent  $t$ . Applying Hensel's lemma, reversing the transformation, and iterating the process yields Algorithm 3.

---

**Algorithm 3** SegmentSplitting
 

---

**Input:**  $g \in K[X, Y]$  irreducible and monic in  $Y$ , with  $g(0, 0) = 0$  and no Puiseux expansions vanishing at  $Y = 0$  outside the origin;  $d \in \mathbb{N}$ .

**Output:** Weierstrass polynomials  $g_1, \dots, g_\ell \in K[[X]][Y]$ , all developed up to  $X$ -degree  $d$ , with  $g = g_1 \cdots g_\ell$  as in (1), and each  $g_i$  corresponding to precisely one Puiseux segment of  $g$  as outlined above.

- 1: let  $t_1, \dots, t_\ell$  be the different initial exponents of the Puiseux expansions of  $g$  (which are obtained from the Newton polygon of  $g$ )
  - 2: **if**  $\ell = 1$  **then**
  - 3:     **return**  $\{g\}$
  - 4:  $t = u/v = \min\{t_1, \dots, t_\ell\}$ , with  $u, v \in \mathbb{N}$
  - 5:  $s = Y$ -degree of  $g$
  - 6:  $F = g(X^v, X^u Y) / X^{su}$
  - 7: compute  $G_0, H_0 \in K[Y]$  with  $H_0 = Y^w$  for some  $w \in \mathbb{N}_{\geq 1}$ ,  $Y \nmid G_0$ , and  $F(0, Y) = G_0 H_0$
  - 8:  $\{G, H\} = \text{HenselLift}(F, G_0, H_0, vd)$
  - 9:  $g_1 = G(X^{1/v}, Y/X^{u/v})$ ,  $h = H(X^{1/v}, Y/X^{u/v})$
  - 10: **return**  $\{g_1\} \cup \text{SegmentSplitting}(h)$
- 

See [9, Theorem 5.1.17] for an alternative approach extending the Weierstrass Division Theorem.

**Example 7.4.** Let  $f = (Y^2 + 2X^3)((Y + 2X^2)^2 + X^5) + Y^6$ . Evaluating  $f$  at  $X = 0$ , we get  $f(0, Y) = (Y^2 + 1)Y^4$ . Applying **SeparateUnit**( $f, 8$ ) gives

$$\begin{aligned} f_0 &= -48X^8Y + 210X^8 + 8X^7Y - 56X^7 - 32X^6Y + 4X^6 + 8X^5Y - X^5 + 12X^4 - 2X^3 - 4X^2Y + Y^2 - 1, \\ g &= 48X^8Y^3 - 46X^8Y^2 + 8X^7Y^3 + 16X^8Y + 8X^7Y^2 - 32X^6Y^3 + 2X^8 + 4X^6Y^2 \\ &\quad + 8X^5Y^3 + 8X^7 + X^5Y^2 + 8X^5Y + 4X^4Y^2 + 2X^3Y^2 + 4X^2Y^3 + Y^4. \end{aligned}$$

The Puiseux expansions of  $g$  are

$$\begin{aligned} \gamma_1 &= a_1 X^{3/2} + a_1 X^{9/2} - 4X^5 + \dots, \\ \gamma_2 &= a_2 X^{3/2} + a_2 X^{9/2} - 4X^5 + \dots, \\ \gamma_3 &= -2X^2 + b_1 X^{5/2} + 16b_1 X^{13/2} + \dots, \\ \gamma_4 &= -2X^2 + b_2 X^{5/2} + 16b_2 X^{13/2} + \dots, \end{aligned}$$

where  $a_1, a_2$  are the roots of  $X^2 + 2$  and  $b_1, b_2$  are the roots of  $X^2 + 1$ .

The smallest initial exponent  $t$  of the expansions is  $t = u/v = 3/2$ . We compute

$$\begin{aligned} F(X, Y) &= g(X^2, X^3Y) = 48X^{13}Y^3 - 8X^{11}Y^3 + 46X^{10}Y^2 + 32X^9Y^3 + 8X^8Y^2 + 8X^7Y^3 \\ &\quad - 16X^7Y - 4X^6Y^2 + X^4Y^2 + 2X^4 + 4X^2Y^2 + 4XY^3 + Y^4 + 8X^2 + 8XY + 2Y^2. \end{aligned}$$

Now,  $F(0, Y) = (Y^2 + 2)Y^2$ . Applying Hensel's lemma to the factors  $Y^2 + 2$  and  $Y^2$ , and reversing the transformation, we obtain

$$\begin{aligned} g_1 &= -4X^6 - 8X^5Y + 2X^3 + Y^2 = (Y^2 + 2X^3) - 8X^5Y - 4X^6, \\ h &= X^5 + 4X^4 + 4X^2Y + Y^2 = (Y + 2X^2)^2 + X^5. \end{aligned}$$

Next, we wish to separate the different blocks in a given Puiseux segment. Consider first blocks inside a segment which have the same initial exponents but whose initial terms are not conjugate. In this case, after applying the above transformation and substituting 0 for  $X$ ,  $F(0, Y)$  will have different factors that do not vanish at the origin, corresponding to each of these blocks. Hence we can still separate these blocks using Hensel's lemma as before.

To be able to separate all blocks, it remains to consider the separation of blocks that have the same initial rational term (and therefore the same initial exponent). Suppose that  $g_1$  is a factor of  $f$  containing some Puiseux blocks of  $f$  all having the same initial terms  $\eta = a_1X^{t_1} + \dots + a_kX^{t_k}$ ,  $a_i \in K, t_i \in \mathbb{N}$ ,  $1 \leq i \leq k$ . In this case, we first apply the transformation  $Y = Y_1 + \eta$ , and compute  $\tilde{g}_1(X, Y_1) = g_1(X, Y_1 + \eta)$ . Then  $\tilde{g}_1$  will contain the same expansions as  $g_1$  but without the initial terms  $\eta$ . We can now proceed as before to separate the blocks. After computing the factors corresponding to each block, we replace  $Y_1$  by  $Y - \eta$  to get the desired factor.

Algorithm 4 summarizes this strategy. In Line 11 of the algorithm, the presence of a power of a linear factor implies that the expansions share a common rational part, and hence it is possible to further split the factor.

---

**Algorithm 4** BlockSplitting

---

**Input:**  $g \in K[X, Y]$  monic of  $Y$ -degree  $s > 0$  such that all the Puiseux expansions of  $g$  are in the same Puiseux segment;  $d \in \mathbb{N}_0$ .

**Output:**  $g_1, \dots, g_r \in K[X, Y]$  such that the expansions of each  $g_i$  are the same as the expansions of the  $i$ -th Puiseux block of  $g$  up to order  $d$  in  $X$ .

```

1:  $L = \emptyset$ 
2:  $\eta$  = the common rational part of all the Puiseux expansions of  $g$ 
3: if  $\eta = 0$  then
4:    $t = u/v$  the initial exponent of the Puiseux expansions of  $g$  (which is obtained from the
     Newton polygon of  $g$ , and by assumption is the same for all expansions)
5:    $\tilde{g}(X, Y) = g(X^v, X^uY)$ 
6:    $F = \tilde{g}/X^{su}$ 
7:   Compute  $G_0, H_0 \in K[Y]$  with  $G_0 \neq 1$  irreducible or a power of an irreducible polynomial
     and  $G_0, H_0$  coprime such that  $F(0, Y) = G_0H_0$ .
8:   if  $H_0 \neq 1$  then
9:      $(G, H) = \text{HenselLift}(F, G_0, H_0, vd)$ 
10:     $g_1 = G(X^{1/v}, Y/X^{u/v}), h = H(X^{1/v}, Y/X^{u/v})$ 
11:    if  $G_0$  is not a power of a linear factor in  $Y$  then
12:      return  $\{g_1\} \cup \text{BlockSplitting}(h)$ 
13:    else
14:      return  $\text{BlockSplitting}(g_1) \cup \text{BlockSplitting}(h)$ 
15:    else
16:      return  $\{g\}$ 
17: else
18:    $\tilde{g} = g(X, Y + \eta)$ 
19:    $\{g_1, \dots, g_r\} = \text{SegmentSplitting}(\tilde{g})$ 
20:   for  $1 \leq i \leq r$  do
21:      $\{h_1, \dots, h_s\} = \text{BlockSplitting}(g_i)$ 
22:      $L = L \cup \{h_1(X, Y - \eta), \dots, h_s(X, Y - \eta)\}$ 
23: return  $L$ 
```

---

The ideas from [9, Theorem 5.1.20] can in some cases also be used for our purpose. However, the cited theorem is not as general as we require.

Our final goal is to separate all factors corresponding to different conjugacy classes of expansions. For this, all algorithms known to us require that we work in algebraic field extensions. We compute the conjugate Puiseux expansions  $\bar{\gamma}_1, \dots, \bar{\gamma}_s$  up to the required degree and then compute the product  $(Y - \bar{\gamma}_1) \cdots (Y - \bar{\gamma}_s)$ . (See Algorithm 10.) This last step is only needed when a Puiseux block contains more than one conjugacy class of expansions.

In Algorithm 5, we sum up the discussion above, arriving at a general splitting algorithm.

---

**Algorithm 5** Splitting
 

---

**Input:**  $f \in K[X, Y]$  irreducible polynomial, monic of  $Y$ -degree  $n$ ;  $d \in \mathbb{N}_0$ .

**Output:**  $f_0$  as in (1) and Weierstrass polynomials  $f_1, \dots, f_r \in K[[X]][Y]$ , all developed up to  $X$ -degree  $d$ , with  $f = f_0 f_1 \cdots f_r$  as in (1), and each  $f_i, 1 \leq i \leq r$  corresponding to precisely one conjugacy class of Puiseux expansions of  $f$  at the origin.

```

1:  $\{f_0, g\} = \text{SeparateUnit}(f, d)$ 
2:  $\{g_1, \dots, g_s\} = \text{SegmentSplitting}(g, d)$ , the factors corresponding to the different Puiseux
   segments of  $g$ 
3: for all  $i = 1, \dots, s$  do
4:   compute  $\{h_1, \dots, h_{s'}\} = \text{BlockSplitting}(g_i, d)$ 
5:   for  $j = 1, \dots, s'$  do
6:     Compute  $\Gamma = \{\gamma_1, \dots, \gamma_\ell\}$ , the singular part of the expansions of  $h_j$ 
7:      $m = \text{number of conjugacy classes in } \Gamma$ 
8:     if  $m > 1$  then
9:       for  $k = 1, \dots, m$  do
10:        Compute  $\Gamma_k = \{\gamma_{k,1}, \dots, \gamma_{k,s_k}\}$ , the expansions of the  $k$ -th conjugacy class of  $\Gamma$ ,
           up to order  $d$  in  $X$ 
11:         $p_k = (Y - \gamma_{k,1}) \cdots (Y - \gamma_{k,s_k})$  developed to degree  $d$ 
12:         $L = L \cup \{p_1, \dots, p_k\}$ 
13:     else
14:        $L = L \cup \{h_j\}$ 
15: return  $L$ .
```

---

**7.5. Integral bases for the branches.** Let  $g \in K[[X]][Y]$  be an irreducible Weierstrass polynomial of degree  $m$ . We show how to algorithmically compute an integral basis for  $\overline{K[[X]][Y]}/\langle g \rangle$  over  $K[[X]]$ . That is, we compute polynomials  $p_1, \dots, p_{m-1} \in K[X][Y]$  as described in Proposition 5.6 and their corresponding integrality exponents.

For each  $d, 0 \leq d \leq m-1$ , we look for a polynomial  $p_d \in K[X][Y]$  of degree  $d$  with maximal valuation at  $g$ .

Let  $\Gamma$  be the set of Puiseux expansions of  $g$ . Since we are assuming  $g$  is irreducible, all the expansions of  $g$  are conjugate.

For any  $d \in \mathbb{N}_0, 0 \leq d < m$ , note that

$$o(\Gamma, d) = \max_{\substack{N \subset \Gamma \\ \#N=d}} \left\{ v_g \left( \prod_{\eta \in N} (Y - \eta) \right) \right\}.$$

Recall that for a given  $N \subset \Gamma$ , we have the formula

$$v_g \left( \prod_{\eta \in N} (Y - \eta) \right) = \min_{\delta \in \Gamma \setminus N} \left\{ \sum_{\eta \in N} v(\delta - \eta) \right\}.$$

To compute  $o(\Gamma, d)$ ,  $1 \leq d < m$ , we do not apply the above formulas but we compute a polynomial  $p_d \in K[X, Y]$  of  $Y$ -degree  $d$  such that  $v_g(p_d) = o(\Gamma, d)$ , recursively truncating the expansions of  $g$ .



We consider first the simple case when there exists  $t \in \mathbb{Q}$  such that the conjugated expansions  $\gamma_1, \dots, \gamma_m$  of  $g$  agree in the terms of degree lower than  $t$  and have conjugate terms  $\alpha_i X^t \in \mathcal{P}_X$ , that is

$$\gamma_i = a_1 X^{d_1} + a_2 X^{d_2} + \dots + a_k X^{d_k} + \alpha_i X^t + \dots$$

where  $a_j \in K$  and  $d_j \in \mathbb{N}_0$ ,  $1 \leq j \leq k$ . To compute the numerator  $p_d$  of the element of degree  $d$  in the integral basis, we truncate  $\gamma_i$  to  $\bar{\gamma}_i$  for  $1 \leq i \leq d$  to degree  $d_k$  and we set

$$p_d = (Y - \bar{\gamma}_1) \cdots (Y - \bar{\gamma}_d) \in K[X, Y].$$

**Lemma 7.5.** *The polynomial  $p_d$  defined above has maximal integrality exponents among all monic polynomials of degree  $d$  in  $Y$ .*

*Proof.* Let  $\tilde{p}_d = (Y - \gamma_{i_1}) \cdots (Y - \gamma_{i_d}) \in \mathcal{P}_X[Y]$ ,  $1 \leq i_1 \leq \dots \leq i_d \leq m$ , be an element of degree  $d$  in  $Y$  of largest valuation at  $g$ . We know that we can always take  $\tilde{p}_d$  in this way. Let  $i'$  be an index not appearing in  $\{i_1, \dots, i_d\}$ . We have by construction

$$v_g(\tilde{p}_d) = v_{\gamma_{i'}}(\tilde{p}_d) = \sum_{j=1}^d v(\gamma_{i'} - \gamma_j) = \sum_{j=1}^d v(\gamma_{i'} - \bar{\gamma}_j) = v_{\gamma_{i'}}(p_d).$$

Since  $\gamma_1, \dots, \gamma_m$  are conjugate and  $p_d \in K[X, Y]$ ,  $v_{\gamma_j}(p_d) = v_{\gamma_{i'}}(p_d)$  for  $1 \leq j \leq m$ . Recall that  $v_g(p_d) = \min_{1 \leq j \leq m} v_{\gamma_j}(p_d)$ . So  $v_g(p_d) = v_g(\tilde{p}_d)$ , as desired.  $\square$

In the general case, when the coefficients  $a_k^{(i)}$  are not all different, the truncation has to be done iteratively. We describe a recursive process to obtain  $p_d$ , the numerator of the integral basis of degree  $d$  in  $Y$ .

Let  $\tilde{p}_d \in \mathcal{P}_X[Y]$  be as in Lemma 7.5. Let  $t_k \in \mathbb{Q}$  be the smallest exponent such that the truncations

$$\gamma_j^{(0)} = a_1^j X^{t_1} + \dots + a_k^j X^{t_k}, \quad t_1 < \dots < t_k$$

of the expansions  $\gamma_j$ ,  $1 \leq j \leq m$ , are pairwise different. We truncate the expansions  $\gamma_j$ ,  $1 \leq j \leq m$ , to degree  $t_{k-1}$ :

$$\gamma_j^{(1)} = a_1^j X^{t_1} + \dots + a_{k-1}^j X^{t_{k-1}}.$$

For the recursion, we define  $g_0 = \prod_{j=1}^m (Y - \gamma_j)$  and  $\bar{g}_0 = \prod_{j=1}^m (Y - \gamma_j^{(1)})$ . Since  $t_k$  was the smallest integer for which all the truncated expansions were different, the expansions  $\gamma_j^{(1)}$ ,  $1 \leq j \leq m$ , can now be grouped into sets of identical expansions, each set having the same number of elements. Denote by  $\eta_1, \dots, \eta_r$  the mutually distinct expansions, and set  $g_1 = (Y - \eta_1) \cdots (Y - \eta_r) \in K[X, Y]$ . By construction  $\bar{g}_0 = g_1^{u_1}$ , with  $u_1 = m/r \in \mathbb{N}$ .

For simplicity, we explain first how to compute recursively the element of degree  $m-1$ , assuming  $\tilde{p}_{m-1} = (Y - \bar{\gamma}_2) \cdots (Y - \bar{\gamma}_m)$ .

We start the  $i$ -th step by applying the whole procedure inductively to  $g_{i-1}$ , computing  $\bar{g}_{i-1}$ ,  $g_i$  and  $u_i$  such that  $\bar{g}_{i-1} = g_i^{u_i}$  and  $\bar{g}_{i-1}$  comes from truncating the expansions of  $g_{i-1}$ . In each step the degree  $r_i$  of  $g_i$  is smaller or equal to the degree  $r_{i-1}$  of  $g_{i-1}$ , and it will be equal to 1 after a finite number  $w$  of steps (bounded by the degree  $t_k$  of the expansions in  $g_0$ ). For that value  $w$ ,  $r_w = 1$  and all the expansions in  $g_w$  are equal. The desired polynomial is

$$p_{s-1} = g_1^{u_1-1} g_2^{u_2-1} \cdots g_w^{u_w-1} \in K[X, Y].$$

We thus obtain Algorithm 6.

**Lemma 7.6.** *With notation as above, let*

$$p_{m-1} = \text{TruncatedFactor}(\{\gamma_1, \dots, \gamma_m\}).$$

*Then  $p_{m-1}$  has maximal valuation at  $g$  over all monic polynomials of degree  $m-1$  in  $Y$ .*



---

**Algorithm 6** Truncated Factor
 

---

**Input:**  $\Delta = \{\gamma_i = a_1^{(i)} X^{t_1} + \dots + a_k^{(i)} X^{t_k}\}_{1 \leq i \leq m}$ , a conjugacy class of Puiseux series of finite length.

**Output:**  $q \in K[X, Y]$  of degree  $m-1$  in  $Y$  such that  $v_{\gamma_1}(q) = v_{\gamma_1}(\tilde{q})$ , with  $\tilde{q} = (Y - \gamma_2) \dots (Y - \gamma_m)$ .

- 1: Let  $\eta_1, \dots, \eta_r$  be the different expansions in the set  $\{\overline{\gamma_1}^{t_k-1}, \dots, \overline{\gamma_m}^{t_k-1}\}$ , the truncations up to degree  $X^{t_k-1}$
  - 2:  $p = (Y - \eta_1) \dots (Y - \eta_r)$
  - 3:  $u = m/r$
  - 4: **if**  $r > 1$  **then**
  - 5:    $p' = \text{TruncatedFactor}(\{\eta_1, \dots, \eta_r\})$
  - 6:   **return**  $q = p^{u-1} p'$ .
  - 7: **else**
  - 8:   **return**  $q = p^{u-1}$ .
- 

*Proof.* As in the proof of Lemma 7.5, it is enough to show that  $v_{\gamma_1}(p_{m-1}) = v_{\gamma_1}(\tilde{p}_{m-1})$ . Let  $\overline{\gamma_2}, \dots, \overline{\gamma_m}$  be the Puiseux expansions of  $p_{m-1}$ , corresponding to truncations of the expansions  $\gamma_2, \dots, \gamma_m$  of  $g$ . By construction,  $v(\gamma_1 - \overline{\gamma_i}) = v(\gamma_1 - \gamma_i)$  for  $i = 2, \dots, m$ . Hence  $v_g(p_{m-1}) = v_{\gamma_1}(p_{m-1}) = v_{\gamma_1}(\tilde{p}_{m-1}) = v_g(\tilde{p}_{m-1})$  as wanted.  $\square$

**Example 7.7.** Returning to Example 4.2, the singular parts of the Puiseux expansions are

$$\begin{aligned}
 \gamma_1^{(0)} &= iX^{3/2} + (-1/2i - 1/2)X^{7/4} + 1/4iX^2 \\
 \gamma_2^{(0)} &= iX^{3/2} + (-1/2i - 1/2)X^{7/4} - 1/4iX^2 \\
 \gamma_3^{(0)} &= iX^{3/2} + (1/2i + 1/2)X^{7/4} + 1/4iX^2 \\
 \gamma_4^{(0)} &= iX^{3/2} + (1/2i + 1/2)X^{7/4} - 1/4iX^2 \\
 \gamma_5^{(0)} &= -iX^{3/2} + (1/2i - 1/2)X^{7/4} + 1/4iX^2 \\
 \gamma_6^{(0)} &= -iX^{3/2} + (1/2i - 1/2)X^{7/4} - 1/4iX^2 \\
 \gamma_7^{(0)} &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4} + 1/4iX^2 \\
 \gamma_8^{(0)} &= -iX^{3/2} + (-1/2i + 1/2)X^{7/4} - 1/4iX^2
 \end{aligned}$$

with  $i^2 = -1$ .

Truncating  $\gamma_i^{(0)}$  to degree  $7/4$  we obtain

$$\begin{aligned}
 \gamma_1^{(1)} &= \gamma_2^{(1)} = iX^{3/2} + (-1/2i - 1/2)X^{7/4} \\
 \gamma_3^{(1)} &= \gamma_4^{(1)} = iX^{3/2} + (1/2i + 1/2)X^{7/4} \\
 \gamma_5^{(1)} &= \gamma_6^{(1)} = -iX^{3/2} + (1/2i - 1/2)X^{7/4} \\
 \gamma_7^{(1)} &= \gamma_8^{(1)} = -iX^{3/2} + (-1/2i + 1/2)X^{7/4}
 \end{aligned}$$

hence  $u_1 = 2$  and

$$\begin{aligned}
 g_1 &= (Y - \gamma_1^{(1)})(Y - \gamma_3^{(1)})(Y - \gamma_5^{(1)})(Y - \gamma_7^{(1)}) \\
 &= Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + 1/4X^7.
 \end{aligned}$$

Applying the whole procedure inductively to  $g_1$  we obtain  $g_2 = Y^2 + X^3$ ,  $u_2 = 2$  and  $g_3 = Y$ ,  $u_3 = 2$ . Combining the factors, we get

$$g = g_1^{u_1-1} g_2^{u_2-1} g_3^{u_3-1} = \left( Y^4 + 2X^3Y^2 + 2X^5Y + X^6 + \frac{1}{4}X^7 \right) (Y^2 + X^3)Y.$$

For computing the elements of any degree  $d$ ,  $1 \leq d \leq m - 1$ , we can easily extend the above construction, leading to Algorithm 7.

---

**Algorithm 7** Truncated Factor General

---

**Input:**  $\Delta = \{\gamma_i = a_1^{(i)} X^{t_1} + \dots + a_k^{(i)} X^{t_k}\}_{1 \leq i \leq m}$ , a conjugacy class of Puiseux series of finite length;  $d \in \mathbb{N}$ ,  $d < m$ .

**Output:**  $p \in K[X, Y]$  of  $Y$ -degree  $d$  such that  $v_{f_\Delta}(p) = v_{f_\Delta}(\tilde{p})$ , with  $\tilde{p}$  the element in  $\mathcal{P}_X[Y]$  of degree  $d$  with maximal valuation at  $f_\Delta$ .

- 1: Set  $\eta_1, \dots, \eta_r$  the different expansions in the set  $\{\overline{\gamma_1^{t_k-1}}, \dots, \overline{\gamma_m^{t_k-1}}\}$
  - 2:  $u = \lfloor d/r \rfloor$ ,  $d' = d - ur$
  - 3: **if**  $d' > 0$  **then**
  - 4:    $g_1 = \text{TruncatedFactorGeneral}(\{\eta_1, \dots, \eta_r\}, d')$
  - 5: **else**
  - 6:    $g_1 = 1$
  - 7: **if**  $u > 0$  **then**
  - 8:    $g = (Y - \eta_1) \cdots (Y - \eta_r)$
  - 9:   **return**  $p = g^u g_1$ .
  - 10: **else**
  - 11:   **return**  $p = g_1$ .
- 

**Lemma 7.8.** *Let  $g \in K[[X]][Y]$  be a Weierstrass polynomial of degree  $m$  in  $Y$ . Let  $\Gamma = \{\gamma_1, \dots, \gamma_m\}$  be the expansions of  $g$  at the origin, which correspond all to the same conjugacy class. Then, for any  $d$ ,  $1 \leq d < m$ , the output  $p_d = \text{TruncatedFactorGeneral}(\Gamma, d)$  is a polynomial with maximal valuation at the origin in the ring  $K[[X]][Y]/\langle g \rangle$  among all polynomials in  $K[X, Y]$  monic of degree  $d$  in  $Y$ .*

*Proof.* Let  $\gamma_1^{(0)}, \dots, \gamma_m^{(0)}$  be the truncations of the Puiseux expansions of  $g$  up to order  $t_k$  and  $g_0, \overline{g_0}, \dots, g_{w-1}, \overline{g_{w-1}}, g_w$  as defined before.

We have noted in Section 4.8 that a polynomial  $p_d$  satisfying the requirements of the lemma can be chosen so that all the Puiseux expansions of  $p_d$  at the origin are truncations of the expansions in  $\Gamma$ . This implies that we can take  $p_d$  to be a product  $p_d = g_1^{d_1} \dots g_w^{d_w}$  of the polynomials  $g_i$  with appropriate exponents. To find the exponents, we note that for all  $i$  the polynomials  $g_{i+1}^{u_{i+1}}$  and  $g_i$  have the same degree, but the valuation of  $g_i$  at  $g$  is larger than the valuation of  $g_{i+1}^{u_{i+1}}$  (since the expansions are developed up to a larger degree). Hence, to construct  $p_d$ , we must first take  $d_1$  as large as possible. Then maximize  $d_2$  and so on iteratively. This is done by Algorithm 7.  $\square$

Setting  $p_d = \text{TruncatedFactorGeneral}(\Gamma, d)$ , we compute  $o(\Gamma, d)$  by the formula

$$o(\Gamma, d) = \sum_{\eta \in N} v(\gamma - \eta),$$

where  $N = \{\eta_1, \dots, \eta_d\}$  are the expansions appearing in  $p_d$  and  $\gamma \in \Gamma$ . (For any expansion  $\gamma \in \Gamma$  the result of the sum is the same, because conjugating the above expression does not modify  $N$ .)

**Example 7.9.** We carry on Example 7.7, computing all the numerators of the elements of the integral basis. We have obtained that the element of the integral basis of degree  $m - 1 = 7$  is the product  $p_7 = g_1 g_2 g_3$ , where  $g_1$ ,  $g_2$  and  $g_3$  have degrees 4, 2 and 1 respectively. To obtain the numerators of the elements of the integral basis of smaller degree  $d$ ,  $1 \leq d \leq 6$ , following Algorithm 7, we have to first take the largest possible power of  $g_1$  so that the total degree is smaller than or equal to  $d$ , then choose the power of  $g_2$  in the same way and finally the power of  $g_3$ . We get the following elements  $p_6 = g_1 g_2$ ,  $p_5 = g_1 g_3$ ,  $p_4 = g_1$ ,  $p_3 = g_2 g_3$ ,  $p_2 = g_2$  and  $p_1 = g_3$ .

The denominators are powers of  $x$ . To obtain the exponents, we compute  $o(\Gamma, d)$  for  $1 \leq d \leq 7$  by looking at the expansions corresponding to each  $g_i$ ,  $i = 1, 2, 3$ , given in Example 7.7. Setting  $N_{g_i}$  the expansions appearing in  $g_i$ ,  $i = 1, 2, 3$ , we have  $\sum_{\eta \in N_{g_1}} v(\gamma - \eta) = 27/4$ ,  $\sum_{\eta \in N_{g_2}} v(\gamma - \eta) = 13/4$  and  $\sum_{\eta \in N_{g_3}} v(\gamma - \eta) = 3/2$  for any  $\gamma \in \Gamma$ . Hence  $o(\Gamma, 1) = 3/2$ ,  $o(\Gamma, 2) = 13/4$ ,  $o(\Gamma, 3) = 13/4 + 3/2 = 19/4$ ,  $o(\Gamma, 4) = 27/4$ ,  $o(\Gamma, 5) = 27/4 + 3/2 = 33/4$ ,  $o(\Gamma, 6) = 27/4 + 13/4 = 10$  and  $o(\Gamma, 7) = 27/4 + 13/4 + 3/2 = 23/2$ . The exponents in the denominators are the integer part of these valuations, hence the integral basis is

$$\left\{ \frac{g_3}{x}, \frac{g_2}{x^3}, \frac{g_2 g_3}{x^4}, \frac{g_1}{x^6}, \frac{g_1 g_3}{x^8}, \frac{g_1 g_2}{x^{10}}, \frac{g_1 g_2 g_3}{x^{11}} \right\}.$$

**7.6. Merging the integral bases for the branches.** We have shown how to compute an integral basis when  $g \in K[[X]][Y]$  is an irreducible Weierstrass polynomial. For the general case when  $g$  is not irreducible, theoretically we can combine all the integral bases of the branches following Corollary 5.10. However, as we discussed in Section 7.1, the use of the extended GCD is not practical. The following result, which extends Corollary 5.10, provides a different strategy replacing the Bézout coefficients from the Euclidean algorithm by more simple and easy to calculate coefficients in  $K[X, Y]$ . These coefficients as well as their integrality exponents can be computed based only on the singular part of the Puiseux expansions of  $f$ .

**Proposition 7.10.** *Let  $A = K[C] = K[X, Y]/\langle f \rangle$ . Let  $f = f_0 f_1 \cdots f_r$  be the factorization of  $f$  in  $K[[X]][Y]$ , where  $f_0 \in K[[X]][Y]$  is a unit in  $K[[X, Y]]$ , and  $f_1, \dots, f_r$  are irreducible Weierstrass polynomials in  $K[[X]][Y]$ . For each  $i = 1, \dots, r$ , let*

$$\mathcal{L}^{(i)} = \left\{ 1 = p_0^{(i)}, \frac{p_1^{(i)}}{X^{e_1^{(i)}}}, \dots, \frac{p_{m_i-1}^{(i)}}{X^{e_{m_i-1}^{(i)}}} \right\}$$

*be an integral basis as in Lemma 5.3 for the normalization of  $K[[X]][Y]/\langle f_i \rangle$ . Let  $h_i = \prod_{j=1, j \neq i}^r f_j$ . Assume  $\beta_i \in K[X, Y]$ ,  $1 \leq i \leq r$ , are such that the order at the origin of  $\beta_i h_i$  in  $K[[X]][Y]/\langle f_i \rangle$  is an integer  $c_i \geq 0$ . Let  $B = K[[X]][Y]/\langle f_1 \cdots f_r \rangle$  and set*

$$\mathcal{B}^{(i)} = \left\{ \frac{\beta_i h_i}{X^{c_i}}, \frac{\beta_i h_i p_1^{(i)}}{X^{c_i + e_1^{(i)}}}, \dots, \frac{\beta_i h_i p_{m_i-1}^{(i)}}{X^{c_i + e_{m_i-1}^{(i)}}} \right\} \subset \overline{B}.$$

*Then  $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$  is a  $K[[X]]$ -module basis of  $\overline{B}$ .*

*Proof.* For fixed  $1 \leq i \leq r$ , by the Bézout identity on  $f_i$  and  $\beta_i h_i$  there exist  $\mu, \nu \in K[[X]][Y]$  and  $e \in \mathbb{Z}_{\geq 0}$  such that  $\mu f_i + \nu \beta_i h_i = X^e$ . Setting  $e_1 = \text{ord}(\nu)$  in  $K[[X]][Y]/\langle f_i \rangle$ , we have  $e = e_1 + c_i$  and  $e_1$  is integer by the hypothesis on  $\beta_i$ . Hence  $\nu/X^{e_1}$  and  $\beta_i h_i/X^{c_i}$  are integral elements over  $K[[X]][Y]/\langle f_i \rangle$ . Call  $g_i = \nu/X^{e_1}$ . Then  $g_i \frac{\beta_i h_i}{X^{c_i}} \equiv \delta_{ij}$  in  $K((X))[Y]/\langle f_j \rangle$ , for  $1 \leq j \leq r$ .

Hence, as in Proposition 5.9, the well defined map of  $K[[X]]$ -modules

$$(t_1 \bmod f_1, \dots, t_r \bmod f_r) \mapsto \sum_{i=1}^r g_i \frac{\beta_i h_i}{X^{c_i}} t_i \bmod f_1 \cdots f_r,$$

maps  $\bigoplus_{i=1}^r \overline{K[[X]][Y]/\langle f_i \rangle}$  isomorphically to  $\overline{K[[X]][Y]/\langle f_1 \cdots f_r \rangle}$ .

For  $1 \leq i \leq r$ , let

$$\mathcal{C}^{(i)} = \left\{ g_i \frac{\beta_i h_i}{X^{c_i}}, g_i \frac{\beta_i h_i p_1^{(i)}}{X^{c_i + e_1^{(i)}}}, \dots, g_i \frac{\beta_i h_i p_{m_i-1}^{(i)}}{X^{c_i + e_{m_i-1}^{(i)}}} \right\}.$$

We first show that as  $K[[X]]$ -modules over  $K[[X]][Y]/\langle f_i \rangle$ ,  $\langle \mathcal{C}^{(i)} \rangle \cong \langle \mathcal{B}^{(i)} \rangle$ . Clearly  $\langle \mathcal{C}^{(i)} \rangle \cong \langle \mathcal{L}^{(i)} \rangle$ , because  $g_i \frac{\beta_i h_i}{X^{c_i}} \equiv 1$ . To see that the  $\langle \mathcal{L}^{(i)} \rangle \cong \langle \mathcal{B}^{(i)} \rangle$ , take  $a \in \langle \mathcal{L}^{(i)} \rangle$ . Then, since  $g_i$  is integral,  $g_i a \in \langle \mathcal{C}^{(i)} \rangle$  and  $a \equiv \frac{\beta_i h_i}{X^{c_i}} g_i a \in \langle \mathcal{B}^{(i)} \rangle$ , proving the isomorphism. It is trivial that  $\langle \mathcal{C}^{(i)} \rangle \cong \langle \mathcal{B}^{(i)} \rangle$  as  $K[[X]]$  modules over  $K[[X]][Y]/\langle f_j \rangle$ ,  $j \neq i$ . Hence  $\langle \mathcal{C}^{(i)} \rangle \cong \langle \mathcal{B}^{(i)} \rangle$  as  $K[[X]]$  modules over  $K[[X]][Y]/\langle f_1 \cdots f_r \rangle$ . Therefore  $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$  is also a  $K[[X]]$ -module basis of  $\overline{B}$ .  $\square$

We address now the computation of coefficients  $\beta_i$ ,  $1 \leq i \leq r$ , with the required property that the order of  $\beta_i h_i$  at  $K[[X]][Y]/\langle f_i \rangle$  is integer. If  $\text{ord}(h_i)$  is integer, we take  $\beta_i = 1$ . In the general case, to find  $\beta_i$  we could use a power of  $h_i$ , since  $\text{ord}(h_i^m) = m \text{ord}(h_i)$ , and we can choose  $m$  so that  $m \text{ord}(h_i)$  is integer. (In fact, we would replace  $h_i$  by  $\bar{h}_i = \prod_{\gamma \in \Delta} (Y - \bar{\gamma})$  where  $\Delta$  are the Puiseux expansions of  $h_i$  and for  $\gamma \in \Delta$ ,  $\bar{\gamma}$  is the singular part of  $\gamma$ , so that we get a polynomial in  $K[X, Y]$  with the same order as  $h_i$  at  $K[[X]][Y]/\langle f_i \rangle$ .) Usually, however, it is more efficient to choose  $\beta_i$  as a product of the factors given by Algorithm 7. We can proceed algorithmically as in Algorithm 8.

---

**Algorithm 8** Merge Coefficients

---

**Input:**  $\Delta_1, \dots, \Delta_r$ , the sets of singular parts of the Puiseux expansions of the conjugacy classes corresponding to the factors  $f_1, \dots, f_r$  of  $f$ .

**Output:**  $\{(\beta_i, c_i)\}_{1 \leq i \leq r}$ ,  $\beta_i \in K[X, Y]$  and  $c_i \in \mathbb{Z}_{\geq 0}$ , such that the order of  $\beta_i h_i$  in  $K[[X]][Y]/\langle f_i \rangle$  at the origin is  $c_i$ , where  $h_i = \prod_{j \neq i} f_j$ .

- 1: **for**  $i = 1, \dots, r$  **do**
  - 2:   **if**  $\text{ord}(h_i) \in \mathbb{Z}$  **then**
  - 3:      $\beta_i = 1$ ,  $c_i = \text{ord}(h_i)$ .
  - 4:   **else**
  - 5:     For each  $1 \leq j \leq r$ ,  $j \neq i$ , and each  $1 \leq k \leq d_j$  ( $d_j$  the degree of  $f_j$ ) set
 
$$f_{j,k} = \text{TruncatedFactorGeneral}(\Delta_j, k)$$
 if  $k < d_j$  and  $f_{j,d_j} = \prod_{\gamma \in \Delta_j} (Y - \bar{\gamma})$ , where  $\bar{\gamma}$  is the singular part of  $\gamma$  as before.
  - 6:     For each prime divisor  $a$  of the denominator of  $\text{ord}(h_i) \in \mathbb{Q}$ , take  $p$  a polynomial of smallest degree in  $Y$  among all the computed polynomials such that the denominator of  $\text{ord}(p)$  is a multiple of  $a$  (note that such polynomials always exist since  $\bar{h}_i$  is a product of some of these polynomials).
  - 7:     Take  $\beta_i$  the product of these factors to appropriate powers. The exponents can be found by solving a linear congruence equation, choosing the solution that minimizes the  $Y$ -degree of  $\beta_i$ .
  - 8:      $c_i = \text{ord}(\beta_i h_i)$ .
  - 9: **return**  $\{(\beta_i, c_i)\}_{1 \leq i \leq r}$ .
- 

To merge the integral basis from the branches applying Proposition 7.10, it remains to truncate the elements  $h_i$ ,  $1 \leq i \leq r$ , to polynomials in  $K[X, Y]$ . Note that the coefficients  $c_i$ ,  $1 \leq i \leq r$ , can be computed from the singular part of the Puiseux expansions of  $f$ . If  $e_c$  is the maximum order of the coefficients  $c_i$ , then we know that for any polynomial appearing in the construction of the integral basis the integrality exponent will be at most  $e_c + E(f)$ . Hence, by Remark 5.4, we can truncate all the numerators to degree  $e_c + E(f)$  in  $X$ . We obtain Algorithm 9.

**Remark 7.11.** To speed up the computation of the integral basis, we first compute the order  $e$  of  $y$  in  $K[X, Y]/\langle g \rangle$  and add the elements  $y^i/x^{\lfloor ei \rfloor}$ ,  $0 \leq i < m = \deg_Y(g)$ , to  $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$ , since those simple elements also belong to the normalization. This is an improvement over Remark 5.4.

**Example 7.12.** Let  $A = K[X, Y]/\langle (Y^3 + X^2)(Y^2 - X^3) + Y^6 \rangle = K[x, y]$  as in Examples 4.5 and 5.11. There are two conjugacy classes of expansions at the origin,  $\Gamma_1 = \{\gamma_1, \gamma_2, \gamma_3\}$  and  $\Gamma_2 = \{\gamma_4, \gamma_5\}$ . We apply Algorithm 8 to compute  $\beta_1$  and hence  $\mathcal{B}^{(1)}$  as in Proposition 7.10. We have  $f_1 = (Y - \gamma_1)(Y - \gamma_2)(Y - \gamma_3)$  and  $h_1 = (Y - \gamma_4)(Y - \gamma_5)$ . The integral basis of  $K[[X]][Y]/\langle f_1 \rangle$  is  $\{1, y, \frac{y^2}{x}\}$ . Evaluating the expansions from  $\Gamma_1$  in  $h_1$ , we see that the order of  $h_1$  at  $f_1$  is  $4/3$ . Applying Algorithm 7 to  $h_1$  we get  $\text{TruncatedFactorGeneral}(h_1, 1) = Y$ . The order of  $y$  at  $f_1$  is  $2/3$ . Hence  $yh_1$  has order 2 at  $f_1$ , which is integer. So we can use  $\beta_1 = Y$ . We get

$$\mathcal{B}^{(1)} = \left\langle \frac{yh_1}{x^2}, \frac{yh_1y}{x^2}, \frac{yh_1y^2}{x^3} \right\rangle.$$

---

**Algorithm 9** Integral basis for Weierstrass polynomial
 

---

**Input:**  $L = \{\{f_1, f_1\}, \dots, \{f_r, f_r\}\}$ , where  $f_i = \{\gamma_{i,1}, \dots, \gamma_{i,m_i}\}$  is the set of singular parts of the  $i$ -th conjugacy class of expansions that vanish at the origin of a polynomial  $f \in K[X, Y]$  monic in  $Y$  and  $f_i$  is the corresponding factor of  $f$ ;  $\{(\beta_1, c_1), \dots, (\beta_r, c_r)\}$ , the output of  $\text{MergeCoefficients}(\{f_1, \dots, f_r\})$ . We assume  $f_i$ ,  $1 \leq i \leq r$ , developed up to  $X$ -degree  $e_c + E(f)$ , with  $e_c = \max_{1 \leq i \leq r} c_i$ .

**Output:**  $\{(p_0, e_0), \dots, (p_{m-1}, e_{m-1})\}$ ,  $p_i \in K[X][Y]$  monic in  $Y$  of degree  $i$  and  $e_i \in \mathbb{Z}_{\leq 0}$ , such that  $\{\frac{p_0}{x^{e_0}}, \dots, \frac{p_{m-1}}{x^{e_{m-1}}}\}$  is an integral basis for the normalization of  $K[[X]][Y]/\langle f_1 \cdots f_r \rangle$ .

- 1:  $m = \deg_Y(f_1 \cdots f_r)$
- 2: **for**  $i = 1, \dots, r$  **do**
- 3:    $h_i = \prod_{j \neq i} f_j$
- 4:   **for**  $d = 0, \dots, m_i - 1$  **do**
- 5:      $q_d = \text{TruncatedFactorGeneral}(f_i, d)$
- 6:      $e(q_d) =$  the integrality exponent of  $q_d$  in  $K[X, Y]/\langle f_i \rangle$ .
- 7:      $p_d = b_i h_i q_d$ ,  $e_d = c_i + e(q_d)$
- 8:      $\mathcal{B}^{(i)} = \left\{ \frac{p_0}{x^{e_0}}, \frac{p_1}{x^{e_1}}, \dots, \frac{p_{m_i-1}}{x^{e_{m_i-1}}} \right\}$
- 9: From  $\mathcal{B}^{(1)} \cup \dots \cup \mathcal{B}^{(r)}$ , compute the integral basis  $\{p_0, p_1/x^{e_1}, \dots, p_{m-1}/x^{e_{m-1}}, \}$ , as indicated in the proof of Lemma 5.3.
- 10: **return**  $\{(p_0, e_0), \dots, (p_{m-1}, e_{m-1})\}$ .

---

This is more simple than using  $b_1 \equiv -2X^2Y^2 - 3X^3 - 2X^2Y + XY^2 - Y^2 - Y$  as in Example 5.11.

We next consider a more complicated example where the coefficient  $\beta_i$  has larger degree.

**Example 7.13.** Let  $f(X, Y) = (Y^6 - 6X^3Y^4 - 2X^7Y^3 + 12X^6Y^2 - 12X^{10}Y - 8X^9)(Y^2 - 2YX^3 - 2X^3)(Y^2 + X^7) + X^{30}$  and  $A = K[X, Y]/\langle f \rangle$ . The Puiseux expansions of  $f$  are

$$\begin{aligned}
 \gamma_1 &= r_1X^{3/2} + X^{7/3} + \dots, & \gamma_6 &= r_2X^{3/2} + r_4X^{7/3} + \dots, \\
 \gamma_2 &= r_1X^{3/2} + r_3X^{7/3} + \dots, & \gamma_7 &= r_1X^{3/2} + X^3 + \dots, \\
 \gamma_3 &= r_1X^{3/2} + r_4X^{7/3} + \dots, & \gamma_8 &= r_2X^{3/2} + X^3 + \dots, \\
 \gamma_4 &= r_2X^{3/2} + X^{7/3} + \dots, & \gamma_9 &= r_5X^{7/2} + \dots, \\
 \gamma_5 &= r_2X^{3/2} + r_3X^{7/3} + \dots, & \gamma_{10} &= r_6X^{7/2} + \dots
 \end{aligned}$$

with  $r_1, r_2$  the roots of  $\lambda^2 - 2 = 0$ ,  $r_3, r_4$  the roots of  $\lambda^2 + \lambda + 1 = 0$  and  $r_5, r_6$  the roots of  $\lambda^2 + 1 = 0$ . They correspond to three conjugacy classes  $\Delta_1 = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$ ,  $\Delta_2 = \{\gamma_7, \gamma_8\}$  and  $\Delta_3 = \{\gamma_9, \gamma_{10}\}$ . We show how to compute  $\beta_1$ . Let  $f_1, f_2$  and  $f_3$  be the Weierstrass polynomials corresponding to each conjugacy class and  $h_1 = f_2f_3$ .

The order of  $h_1$  at  $f_1$  is  $41/6$  (recall that the order of  $h_1$  at  $f_1$  is the order in  $X$  of  $(\gamma - \gamma_7) \cdots (\gamma - \gamma_{10})$  for any expansion  $\gamma$  of  $h_1$ ). Applying Algorithm 7 to  $\Delta_2$  and  $\Delta_3$  for  $c = 1, 2$  we get the polynomials  $\{y, y^2 - 2yx^3 - 2x^3\}$  and  $\{y, y^2 + x^7\}$ . We have  $\text{ord}_{f_1}(y) = 3/2$ ,  $\text{ord}_{f_1}(y^2 - 2yx^3 - 2x^3) = 23/6$ ,  $\text{ord}_{f_1}(y^2 + x^7) = 3$ .

We can take  $\beta_1 = y^{e_1}(y^2 - 2yx^3 - 2x^3)^{e_2}$  for appropriate  $e_1, e_2 \in \mathbb{N}_0$ . The exponents must satisfy the equation  $e_1 \frac{3}{2} + e_2 \frac{23}{6} + \frac{41}{6} \in \mathbb{Z}$ . The corresponding linear congruence equation is  $9e_1 + 23e_2 + 41 \equiv 0(6)$ . The solution that minimizes the  $Y$ -degree of  $\beta_i$  is  $e_1 = 1$  and  $e_2 = 2$ . We get  $\beta_1 = y(y^2 - 2yx^3 - 2x^3)^2$ .

**7.7. Ad-hoc Algorithm for the Case of one Characteristic Exponent.** We describe an algorithm, which allows us to write down an integral basis directly in the case of a singularity with only one conjugacy class of Puiseux expansions.

**Lemma 7.14.** *Let  $f \in K[[x]][y]$  be an irreducible Weierstrass polynomial with respect to  $y$  and  $\deg_y f = n$ . Let  $y(x)$  be a Puiseux expansion, and  $y(x) = \sum_{i \geq m} a_i x^{\frac{i}{n}}$ ,  $a_m \neq 0$ ,  $m > n$  and  $\gcd(m, n) < n$ . Let  $k_0 = n$ ,  $k_1 = m$ ,  $k_2, \dots, k_g$  be the characteristic exponents and let  $\varepsilon$  be a primitive  $n$ -th root of unity. The following holds (cf. [9, Lemma 5.2.18(1)] and the proof thereof):*

$$(1) \quad f = \prod_{i=1}^n (y - y(\varepsilon^i x))$$

(2) For  $j = 1, \dots, g$  denote by  $N_j$  the set of all  $i \in \{1, \dots, n\}$  such that

$$\frac{k_0}{\gcd(k_0, \dots, k_{j-1})} \mid i \quad \text{and} \quad \frac{k_0}{\gcd(k_0, \dots, k_j)} \nmid i.$$

Then

$$\text{ord}_x(y(x) - y(\varepsilon^i x)) = \frac{k_j}{n}$$

for all  $i \in N_j$ . In particular, if  $g = 1$  then

$$\text{ord}_x(y(x) - y(\varepsilon^i x)) = \frac{k_1}{n}$$

if  $i$  is not a multiple of  $n$ .

(3) We have

$$\begin{aligned} \text{ord}_x \frac{\partial f}{\partial y}(x, y(x)) &= \sum_{j=1}^g (\gcd(k_0, \dots, k_{j-1}) - \gcd(k_0, \dots, k_j)) \frac{k_j}{n} \\ &= \text{Int}_{\{1, \dots, \hat{i}, \dots, n\}} \end{aligned}$$

for all  $i$ .

**Proposition 7.15.** *With notation as above we have:*

(1) For  $e = \left\lfloor \text{ord}_x \frac{\partial f}{\partial y}(x, y(x)) \right\rfloor$  the element  $\frac{\partial f}{x^e}$  is integral over  $K[[x]]$  and  $e$  is maximal.

(2) Let

$$e = \left\lfloor \text{ord}_x \frac{\partial^{n-1} f}{\partial y^{n-1}}(x, y(x)) \right\rfloor.$$

Then  $\frac{\partial^{n-1} f}{\partial y^{n-1} x^e}$  is integral over  $K[[x]]$ ,  $e = \left\lfloor \frac{k_1}{n} \right\rfloor$  and  $e$  is maximal.

(3) If  $g = 1$  then

$$1, \frac{\partial^{n-1} f}{\partial y^{n-1} x^{e_1}}, \dots, \frac{\partial f}{\partial y x^{e_{n-1}}}$$

with

$$e_i = \left\lfloor \text{ord}_x \frac{\partial^{n-i} f}{\partial y^{n-i}}(x, y(x)) \right\rfloor$$

form an integral basis of  $\overline{K[[x, y]] / (f)}$  over  $K[[x]]$ .

We now prove Proposition 7.15.

*Proof.* Choose  $\Omega \subseteq \{1, \dots, n\}$  with  $|\Omega| = d$  and  $\text{Int}_\Omega$  maximal. Then

$$\bar{p} := \prod_{j \in \Omega} (y - y(\varepsilon^j x))$$

is a polynomial of degree  $d$  with respect to  $y$  and  $\text{ord}_x \bar{p}(x, y(x))$  is maximal. Let

$$e = \left\lfloor \text{ord}_x \bar{p}(x, y(x)) \right\rfloor.$$

By Lemma 7.8, for some approximation  $p$  of  $\bar{p}$ , we can choose  $\frac{p(x, y)}{x^e}$  as the degree  $d$  element in the integral basis.

We obtain (1) for  $d = n - 1$  and (2) for  $d = 1$ , and  $\text{Int}_\Omega$  is independent of  $\Omega$ . The same holds true for (3) in case  $g = 1$ .  $\square$

**Remark 7.16.** If  $f = y^4 - 2x^3y^2 - 4x^{11}y + x^6 - x^{19}$  then  $y(x) = x^{\frac{6}{4}} + x^{\frac{19}{4}}$  is a Puiseux expansion,  $g = 2$  and (3) in Proposition 7.15 does not hold.

*Proof.* We compute  $\left\lfloor \text{ord}_x \frac{\partial^2 f}{\partial y^2}(x, y(x)) \right\rfloor = 4$ . However,

$$\bar{p} = (y - y(-x))(y - y(ix))$$

gives  $\lfloor \text{ord}_x \bar{p}(x, y(x)) \rfloor = 6$ .  $\square$

**7.8. Computation of the Local Contribution to the Integral Basis.** Finally, assuming that  $P = \langle X, Y \rangle$  is the only singularity at  $X = 0$ , we compute the local contribution to the integral basis from the integral basis of  $K[[X]][Y]/\langle f_1 \cdots f_r \rangle$  using Proposition 6.1. We describe the complete procedure in Algorithm 10.

---

**Algorithm 10** Local contribution to the integral basis

---

**Input:**  $f \in K[X, Y]$  irreducible polynomial, monic of  $Y$ -degree  $n$ , with only one singularity at  $X = 0$ , located at the origin.

**Output:** A basis of the minimal local contribution of  $K[X, Y]/\langle f \rangle$  at the origin.

- 1: Compute  $\Delta_0$  the set of the singular parts of the Puiseux expansions of  $f$  at  $X = 0$  that do not vanish at the origin and  $\Delta_1, \dots, \Delta_r$  the sets of singular parts of the conjugacy classes of Puiseux expansions of  $f$  at  $X = 0$  that vanish at the origin.
  - 2: Compute  $E(f)$  as indicated in Section 4.8.
  - 3: Compute  $\{(\beta_i, c_i)\}_{1 \leq i \leq r} = \text{MergeCoefficients}(\{\Delta_1, \dots, \Delta_r\})$ .
  - 4:  $e_c = \max_{1 \leq i \leq r} c_i$ .
  - 5:  $\{f_0, f_1, \dots, f_r\} = \text{Splitting}(f, E(f) + e_c)$ , where  $f_0$  corresponds to  $\Delta_0$  and  $f_1, \dots, f_r$  correspond to  $\Delta_1, \dots, \Delta_r$ .
  - 6:  $m_0 = \deg(f_0)$ ,  $m = n - m_0$
  - 7:  $\{(p'_0, e'_0), \dots, (p'_m, e'_m)\} = \text{IntegralBasisForWeierstrassPolynomial}(\{(\Delta_1, f_1), \dots, (\Delta_r, f_r)\}, \{(\beta_1, c_1), \dots, (\beta_r, c_r)\})$
  - 8: **for**  $i = 0, \dots, \deg(f_0) - 1$  **do**
  - 9:      $p_i = y^i$ ,  $e_i = 1$
  - 10: **for**  $i = 0, \dots, m - 1$  **do**
  - 11:      $p_{m_0+i} = f_0 \cdot p'_i$ ,  $e_{m_0+i} = e'_i(i)$
  - 12: **return**  $\mathcal{B} = \{p_0/x^{e_0}, \dots, p_{n-1}/x^{e_{n-1}}\}$ .
- 

To compute a (global) integral basis of  $\bar{A}$  over  $K[x]$  we can now use Proposition 3.1.

**Remark 7.17.** In the presence of conjugated singularities, to get a better performance, our local algorithm can handle groups of conjugate singularities simultaneously, in a similar way as in [21, Section 4]. If  $I \subset K[X, Y]$  is an associated prime of the singular locus, corresponding to a group of conjugate singularities, we apply a linear coordinate change if necessary, so that no two of these singularities have the same  $X$ -coordinate. Then we can find polynomials  $q_1, q_2 \in K[X]$  such that  $I = \langle q_1(X), Y - q_2(X) \rangle$ . We take  $\alpha$  a root of  $q_1(X)$  and translate the singularity  $(\alpha, q_2(\alpha))$  to the origin. We compute the local contribution to integral basis at the origin and apply the inverse translation to the output. The common denominator of the resulting generators will be a power of  $x - \alpha$ . We replace  $(x - \alpha)$  by  $q_1(x)$  in the denominators and we eliminate  $\alpha$  from the numerators by considering  $\alpha$  as a new variable and reducing each numerator by the numerators of smaller degree (written all with the same common denominator), using an elimination ordering  $\alpha \gg y \gg x$ . Since an integral basis over the original ring always exists, the elimination process is guaranteed to eliminate  $\alpha$  from the numerators.



**Example 7.18.** Let  $A = K[X, Y]$  and  $f(X, Y) = Y^3 - (X^2 - 2)^2$ . The singular locus contains only one primary component  $\langle X^2 - 2, Y^2 \rangle$ , with radical  $\langle X^2 - 2, Y \rangle$ . It consists of the two conjugated points  $(-\sqrt{2}, 0)$  and  $(\sqrt{2}, 0)$ . We take  $\alpha = \sqrt{2}$  and compute the local contribution at  $(\alpha, 0)$  translating that point to the origin. After the inverse translation, we get the integral basis of the local contribution  $\left\{1, y, \frac{y^2}{x-\alpha}\right\}$ .

The local contribution to the integral basis at the conjugate singularity is  $\left\{1, y, \frac{y^2}{x+\alpha}\right\}$ . Hence the global integral basis is  $\left\{1, y, \frac{y^2}{x^2-2}\right\}$ . (In this simple case, we did not need to eliminate  $\alpha$  from the numerator.)

**Example 7.19.** Let  $A = K[X, Y]$  and  $f(X, Y) = (Y - X)^3 - (X^2 - 2)^2$ . Now the radical of the singular locus is the prime ideal  $\langle X^2 - 2, Y - X \rangle$ . It consists of the two conjugated points  $(-\sqrt{2}, -\sqrt{2})$  and  $(\sqrt{2}, \sqrt{2})$ . We take  $\alpha = \sqrt{2}$  and compute the local contribution at  $(\alpha, \alpha)$ . We get the integral basis of the local contribution

$$\left\{1, y, \frac{y^2 - 2\alpha y + 2}{x - \alpha}\right\}.$$

To eliminate  $\alpha$  from the last numerator, we write all the fractions with the same denominator  $\left\{\frac{x-\alpha}{x-\alpha}, \frac{y(x-\alpha)}{x-\alpha}, \frac{y^2-2\alpha y+2}{x-\alpha}\right\}$ , and we can now reduce the last one to get  $\left\{1, y, \frac{y^2-2xy+2}{x-\alpha}\right\}$ . Hence the global integral basis is  $\left\{1, y, \frac{y^2-2xy+2}{x^2-2}\right\}$ .

## 8. TIMINGS

We present timings, comparing the implementation of our integral basis algorithm<sup>2</sup> in SINGULAR with obtaining an integral basis via the local normalization algorithm<sup>3</sup> outlined in Section 3, with the implementation of van Hoeij's algorithm<sup>4</sup> in MAPLE [18] and with the implementation of the variant of the Round 2 algorithm<sup>5</sup> in MAGMA [6, 14].

We compute integral bases for  $A = \mathbb{Q}[X, Y]/\langle f \rangle$  with polynomials  $f$  as specified. All timings are in seconds, taken on an AMD Opteron 6174 machine with 48 cores, 2.2GHz, and 128GB of RAM running a Linux operating system. A dash indicates that the computation did not finish within 6000 seconds. We only use parallel computations for the decomposition of the singular locus. The parallelization of the integral basis algorithm and a modular approach following the strategy of [3] is subject to ongoing work. Recall that for obtaining the integral bases, singularities at infinity of the curve  $\{f = 0\}$  do not matter.

**8.1. One Singularity of Type A.** The plane curves with defining equation  $f(X, Y) = Y^2 + X^{k+1} + Y^d$ ,  $k \geq 1$ ,  $d \geq 3$  have exactly one singularity at the origin, which is of type  $A_k$ .

$k$	$d$	SINGULAR		MAPLE	MAGMA
		INTBAS	NORMAL		
5	10	0	0	0	0
5	100	0	0	1	168
5	500	0	1	49	*
50	60	0	0	1	294
50	100	0	1	2	10751
50	500	0	0	76	*
90	100	0	1	4	*
90	500	0	1	102	*
400	500	0	3	346	*

<sup>2</sup>column SINGULAR INTBAS in the tables

<sup>3</sup>column SINGULAR NORMAL in the tables

<sup>4</sup>column MAPLE in the tables

<sup>5</sup>column MAGMA in the tables

**8.2. One Singularity of Type D.** The plane curves with defining equation  $f(X, Y) = X(X^{k-1} + Y^2) + Y^d$ ,  $k \geq 3$ ,  $d \geq 3$  have exactly one  $D_{k+1}$ -singularity at the origin.

$k$	$d$	SINGULAR		MAPLE	MAGMA
		INTBAS	NORMAL		
5	10	0	0	0	0
5	100	0	1	1	1683
5	500	3	0	53	*
50	60	0	1	6	312
50	100	0	1	17	3480
50	500	3	1	808	*
90	100	0	1	51	*
90	500	3	1	103	*
400	500	3	4	2326	*

**8.3. Ordinary Multiple Points.** We consider random curves of degree  $d$  with an ordinary  $k$ -fold point at the origin. The defining polynomials were generated by the function `polyDK` from the SINGULAR library `integralbasis.lib` (using the random seed 1231).

$k$	$d$	SINGULAR		MAPLE	MAGMA
		INTBAS	NORMAL		
5	10	0	2	0	0
15	20	0	7784	1	4
15	30	1	*	28	124
20	25	0	*	2	18
20	30	1	*	19	42

**8.4. Curves With Many Singularities of Type A.** The plane curves with defining equations

$$f_{5,n} = X^{2n} + Y^{2n} + Z^{2n} + 2(X^n Z^n - X^n Y^n + Y^n Z^n)$$

were given in [7] and have  $3n$  singularities of type  $A_{n-1}$  if  $n$  is odd. We substitute  $Z = X - 2Y + 1$ .

$n$	SINGULAR		MAPLE	MAGMA
	INTBAS	NORMAL		
5	0	1249	1	1
7	1	*	7	8
9	18	*	30	59
11	56	*	231	251

**8.5. More General Singularities.** We now consider some examples of curves which have singularities of a type other than  $ADE$  or ordinary multiple points:

- (1)  $f = -X^{15} + 21X^{14} - 8X^{13}Y + 6X^{13} + 16X^{12}Y - 20X^{11}Y^2 + X^{12} - 8X^{11}Y + 36X^{10}Y^2 - 24X^9Y^3 - 4X^9Y^2 + 16X^8Y^3 - 26X^7Y^4 + 6X^6Y^4 - 8X^5Y^5 - 4X^3Y^6 + Y^8$ : one singularity at the origin with multiplicity  $m = 8$  and delta invariant  $\delta = 42$ , a node, and a set of 6 conjugate nodes.
- (2)  $f = (Y^4 + 2X^3Y^2 + X^6 + X^5Y)^3 + X^{11}Y^{11}$ : one singularity at the origin with  $m = 12$  and  $\delta = 133$ .
- (3)  $f = (Y^5 + Y^4X^7 + 2X^8)(Y^3 + 7X^4)(Y^7 + 2X^{12})(Y^{11} + 2X^{18}) + Y^{30}$ : one singularity at the origin with  $m = 26$  and  $\delta = 523$ .
- (4)  $f = (Y^{15} + 2X^{38})(Y^{19} + 7X^{52}) + Y^{36}$ : one singularity at the origin with  $m = 34$  and  $\delta = 1440$ .
- (5)  $f = (Y^{15} + 2X^{38})(Y^{19} + 7X^{52}) + Y^{100}$ : higher degree, but same type of singularity.
- (6)  $f = Y^{40} + XY^{13} + X^4Y^5 + X^5 + 2X^4 + X^3$ : one double point with  $\delta = 2$  and one triple point with  $\delta = 19$  (see [21, Section 6.1]).
- (7)  $f = Y^{200} + XY^{13} + X^4Y^5 + X^5 + 2X^4 + X^3$ : higher degree, but same type of singularity.
- (8)  $f = (Y^{35} + Y^{34}X^7 + 2X^{38})(Y^{33} + 7X^{44})(Y^{37} + 2X^{52}) + Y^{110}$ : one singularity at the origin with  $m = 105$  and  $\delta = 6528$ .

No.	$y$ -degree	SINGULAR		MAPLE	MAGMA
		INTBAS	NORMAL		
(1)	8	0	*	0	0
(2)	12	9	*	1	1
(3)	30	11	*	5	31
(4)	36	1	*	5	59
(5)	100	1	*	34	*
(6)	40	0	2	1	9
(7)	200	1	3	12	*
(8)	110	*	*	*	*

In Example (8), SINGULAR and MAPLE do not finish due to the computation of the decomposition of the singular locus of the curve. See Section 8.6 for the timings of the computation of the local contribution to the integral basis at the origin.

We note that in most cases, our proposed algorithm is much faster than the algorithms implemented in MAPLE and MAGMA.

**8.6. Detailed Analysis of Some Examples.** The computation of an integral basis with our algorithm has two major components. First, we decompose the singular locus into associated primes, secondly we compute the local contribution to the integral basis at each associated prime and then we merge the results.

In MAPLE a similar strategy is followed, computing first all the  $x$ -coordinates of the singular points. This first step is part of both integral basis approaches, and can be time consuming in some examples. To analyze in more detail the difference between the integral basis computations, we provide here timings for the computation of the integral basis at the origin for some examples where the origin is the only singularity. This can be specified in SINGULAR and MAPLE by certain input options.

Example	$k$	$d$	SINGULAR	MAPLE
			INTBAS	
8.1	5	500	0	49
8.1	50	500	0	75
8.1	400	500	0	346
8.2	5	500	2	49
8.2	50	500	2	571
8.2	400	500	2	1575
8.3	15	30	0	26
8.3	20	25	0	2
8.3	20	30	1	17
8.5 (2)			9	1
8.5 (3)			4	2
8.5 (5)			1	16
8.5 (8)			25	1483

We observe that for the examples in Section 8.1 the time required for the singular locus decomposition is not significant. For the examples in Section 8.2, MAPLE uses a significant amount of time for this task, but still the most time consuming part is the computation of the integral basis at the origin. For the examples in Section 8.3, in our implementation most of the time is used for computing the decomposition of the singular locus. The computation of the integral basis at the origin is significantly faster than in MAPLE. For the examples in Section 8.5 various situations occur. In Example 8.5 (2) the time for the initial decomposition was not significant, and computation of the integral basis at the origin in our implementation

is slower than MAPLE. In this example, the algorithm runs into an algebraic field extension of high degree. At current state, the handling of such extensions in SINGULAR is not optimal.

## REFERENCES

- [1] Shreeram S. Abhyankar. *Algebraic geometry for scientists and engineers*. Providence, RI: American Mathematical Society, 1990.
- [2] Elizabeth A. Arnold. Modular algorithms for computing Gröbner bases. *J. Symbolic Comput.*, 35(4):403–419, 2003.
- [3] Janko Böhm, Wolfram Decker, Claus Fieker, and Gerhard Pfister. The use of bad primes in rational reconstruction. *Math. Comp.*, 84(296):3013–3027, 2015.
- [4] Janko Böhm, Wolfram Decker, Santiago Laplagne, and Gerhard Pfister. Local to global algorithms for the Gorenstein adjoint ideal of a curve. 2015. <http://arxiv.org/abs/1505.05040>.
- [5] Janko Böhm, Wolfram Decker, Santiago Laplagne, Gerhard Pfister, Andreas Steenpaß, and Stefan Steidel. Parallel algorithms for normalization. *J. Symbolic Comput.*, 51:99–114, 2013.
- [6] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I: The user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.
- [7] José Ignacio Cogolludo. Fundamental group for some cuspidal curves. *Bull. London Math. Soc.*, 31(2):136–142, 1999.
- [8] Theo de Jong. An algorithm for computing the integral closure. *J. Symbolic Comput.*, 26(3):273–277, 1998.
- [9] Theo de Jong and Gerhard Pfister. *Local analytic geometry. Basic theory and applications*. Braunschweig: Vieweg, 2000.
- [10] Wolfram Decker, Theo de Jong, Gert-Martin Greuel, and Gerhard Pfister. The normalization: a new algorithm, implementation and comparisons. In *Computational methods for representations of groups and algebras (Essen, 1997)*, volume 173 of *Progr. Math.*, pages 177–185. Birkhäuser, Basel, 1999.
- [11] Wolfram Decker, Gert-Martin Greuel, G. Pfister, and H. Schönemann. SINGULAR 4-0-2 — A computer algebra system for polynomial computations. 2015. <http://www.singular.uni-kl.de>.
- [12] Clémence Durvy. *Algorithmes pour la décomposition primaire des idéaux polynomiaux de dimension nulle donnés en évaluation*. PhD thesis, Université de Versailles - Saint-Quentin, 2008.
- [13] David Eisenbud. *Commutative algebra. With a view toward algebraic geometry*. Berlin: Springer, 1995.
- [14] David Ford and Pascal Letard. Implementing the round four maximal order algorithm. *J. Théor. Nombres Bordeaux*, 6(1):39–80, 1994.
- [15] Hans Grauert and Reinhold Remmert. *Analytische Stellenalgebren. Unter Mitarbeit von O. Riemenschneider*. Berlin: Springer, 1971.
- [16] Gert-Martin Greuel, Santiago Laplagne, and Frank Seelisch. Normalization of rings. *J. Symbolic Comput.*, 45(9):887–901, 2010.
- [17] Gert-Martin Greuel and Gerhard Pfister. *A Singular introduction to commutative algebra. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann. 2nd extended ed.* Berlin: Springer, 2007.
- [18] Michael B. Monagan, Keith O. Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron, and Paul DeMarco. *Maple 18 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2014.
- [19] Henning Stichtenoth. *Algebraic function fields and codes. 2nd ed.* Berlin: Springer, 2nd ed. edition, 2009.
- [20] Irena Swanson and Craig Huneke. *Integral closure of ideals, rings, and modules*. Cambridge: Cambridge University Press, 2006.
- [21] Mark van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *J. Symbolic Comput.*, 18(4):353–363, 1994.

JANKO BÖHM, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF KAISERSLAUTERN, ERWIN-SCHRÖDINGER-STR., 67663 KAISERSLAUTERN, GERMANY  
*E-mail address:* boehm@mathematik.uni-kl.de

WOLFRAM DECKER, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF KAISERSLAUTERN, ERWIN-SCHRÖDINGER-STR., 67663 KAISERSLAUTERN, GERMANY  
*E-mail address:* decker@mathematik.uni-kl.de

SANTIAGO LAPLAGNE, DEPARTAMENTO DE MATEMÁTICA, FCEN, UNIVERSIDAD DE BUENOS AIRES - CIUDAD UNIVERSITARIA, PABELLÓN I - (C1428EGA) - BUENOS AIRES, ARGENTINA  
*E-mail address:* slaplagn@dm.uba.ar

GERHARD PFISTER, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF KAISERSLAUTERN, ERWIN-SCHRÖDINGER-STR., 67663 KAISERSLAUTERN, GERMANY  
*E-mail address:* pfister@mathematik.uni-kl.de